Claude prende il controllo del computer

Allinea

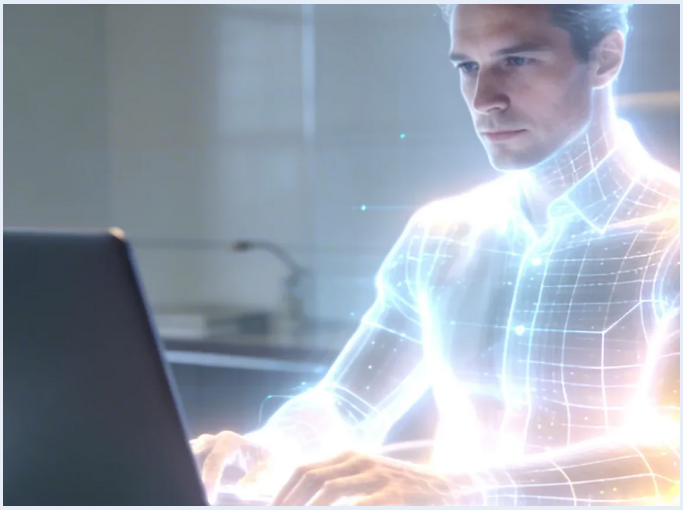
Avvera Compliance Review

Aprile 2026

Allinea
Avvera Compliance Review
Aprile 2026

Claude prende il controllo del computer: Anthropic lancia il "computer use"

Il 23 Aprile 2026 Anthropic ha annunciato una delle funzionalità più ambiziose mai rilasciate per Claude: la possibilità di controllare il computer dell'utente in modo autonomo, eseguendo compiti in sua assenza. Disponibile in research preview per i sottoscrittori dei piani Claude Pro e Max, la funzione si integra con Dispatch, lo strumento mobile lanciato la settimana precedente che consente di assegnare compiti a Claude direttamente dallo smartphone. Il risultato è un sistema in cui l'utente parte, lascia un'istruzione, e trova il lavoro fatto al ritorno.



Come funziona

Quando Claude riceve un compito da eseguire, verifica innanzitutto se dispone dei connettori necessari per completarlo - ad esempio Google Calendar o Slack. Se non li ha, passa al controllo diretto del computer, navigando lo schermo come farebbe un essere umano. Può aprire applicazioni, navigare il browser, compilare fogli di calcolo e gestire file complessi, il tutto senza alcuna configurazione preliminare da parte dell'utente. Il caso dimostrativo scelto da Anthropic è eloquente: un utente in ritardo per una riunione chiede a Claude di esportare un pitch deck in PDF e allegarlo all'invito del calendario. Claude esegue il compito autonomamente, senza che l'utente tocchi il computer. Non è fantascienza: è una research preview disponibile oggi, anche se per ora limitata ai computer Mac, con Windows e Linux non ancora supportati.

" Anthropic ha implementato misure per bloccare azioni non autorizzate "

Il contesto competitivo: la corsa agli agenti AI

L'annuncio arriva in un momento in cui la competizione nel settore degli agenti AI si è intensificata dopo la rapida ascesa di OpenClaw, che ha attirato l'attenzione del settore per funzionalità simili. OpenClaw consente agli utenti di inviare istruzioni tramite WhatsApp o Telegram per eseguire compiti sul computer locale. Il CEO di Nvidia Jensen Huang lo ha definito la prossima grande evoluzione dopo ChatGPT, mentre OpenAI ha assunto il suo creatore, Peter Steinberger, per accelerare il lavoro sugli agenti personali. La versione di Anthropic è più controllata rispetto a OpenClaw: adotta un approccio permission-first, richiedendo l'autorizzazione dell'utente prima di accedere a una nuova applicazione, e per ora è disponibile solo su Mac. La scelta di un approccio più cauto è coerente con il posizionamento di Anthropic come azienda orientata alla sicurezza dell'AI - ma in un mercato in cui la velocità di adozione conta, la prudenza ha anche un costo competitivo.

I profili di rischio

Anthropic non nasconde i limiti della funzione. "Il computer use è ancora in una fase iniziale rispetto alla capacità di Claude di programmare o interagire con il testo", ha dichiarato la società. "Claude può commettere errori, e mentre continuiamo a migliorare le nostre misure di sicurezza, le minacce continuano a evolversi." Dal punto di vista della sicurezza informatica e della protezione dei dati, le implicazioni sono rilevanti. Un agente AI che controlla il computer ha accesso potenzialmente illimitato a file, applicazioni e dati personali. Anthropic ha implementato misure per bloccare azioni non autorizzate come l'accesso a siti bancari o l'inserimento di credenziali sensibili, e raccomanda di monitorare l'attività del dispositivo per rilevare accessi non autorizzati.

Claude prende il controllo del computer: Anthropic lancia il "computer use"

Resta però aperta la questione di come questi sistemi si collochino rispetto al GDPR: un agente AI che processa documenti, naviga applicazioni e interagisce con servizi di terze parti sul computer di un dipendente è, a tutti gli effetti, uno strumento di trattamento di dati personali. Chi è il titolare del trattamento? Quali dati vengono trasmessi ai server di Anthropic durante l'esecuzione dei compiti? Le risposte non sono ancora nella documentazione pubblica.

Conclusioni
Il "computer use" di Claude segna un passaggio qualitativo nel panorama degli assistenti AI: da strumenti che rispondono a strumenti che agiscono. Anche altre aziende stanno percorrendo questa strada, come dimostra la spinta di Microsoft su Copilot, ma Anthropic è tra le prime a portare questa capacità in un prodotto consumer con un approccio strutturato alla sicurezza. Per gli utenti, la promessa è concreta: delegare a Claude compiti ripetitivi e recuperare tempo. Per le aziende e i professionisti che trattano dati sensibili, la domanda da porsi prima di abilitare la funzione è altrettanto concreta: siamo sicuri di sapere cosa vede Claude mentre lavora per noi?

Allinea
Avvera Compliance Review
Aprile 2026

Meta e Google davanti alla giuria: quando il design diventa responsabilità

Nel giro di ventiquattro ore, Meta ha subito due condanne in due diversi tribunali americani. Un tribunale del New Mexico l'ha sanzionata con 375 milioni di dollari per non aver protetto i minori dai predatori sessuali sulle proprie piattaforme.
Una giuria di Los Angeles ha condannato Meta e Google a risarcire con 3 milioni di dollari una donna che aveva accusato le due società per una dipendenza dai social network sviluppata durante l'infanzia, che aveva generato in lei ansia, depressione e problemi legati alla sua immagine corporea. Due verdetti distinti, un messaggio unitario: il terreno della responsabilità delle piattaforme digitali si sta spostando, e lo spostamento è strutturale.

La strategia che ha cambiato tutto: dal contenuto al design
L'accusa ha costruito la propria strategia per superare lo scudo della Section 230, evitando di concentrarsi sui contenuti e spostando invece l'attenzione sulle scelte di progettazione dei servizi. È questa la mossa che rende il processo californiano storicamente rilevante. Anziché contestare ciò che gli utenti pubblicano - terreno su cui le piattaforme hanno difese consolidate - l'accusa ha qualificato Instagram e YouTube come prodotti progettati con caratteristiche in grado di trattenere l'attenzione e incentivare un uso compulsivo, soprattutto tra i più giovani. Tra queste caratteristiche: la possibilità di scorrere all'infinito, la riproduzione automatica dei video, i suggerimenti algoritmici di contenuti e i filtri per modificare le foto, accusati di acuire problemi psicologici legati al rapporto con il proprio corpo. Il parallelo con l'industria del tabacco non è casuale. Il processo ha preso spunto dalle strategie accusatorie utilizzate negli anni Novanta contro le principali società produttrici di sigarette: anche loro furono accusate di non aver posto rimedio agli effetti negativi dei loro prodotti pur essendone al corrente. Le società di sigarette dovettero risarcire alcuni clienti per centinaia di miliardi di dollari e accettare modifiche alle pratiche di marketing, contribuendo a una diminuzione nel consumo.

Meta e Google davanti alla giuria: quando il design diventa responsabilità

" I danni punitivi riconosciuti hanno una funzione segnaletica più che risarcitoria"

Il punto debole della difesa: i documenti interni
Nel corso del processo sono emersi materiali interni che mostrano come le aziende fossero consapevoli degli effetti di alcune scelte di design, in particolare su utenti più giovani. Zuckerberg ha riconosciuto che in passato il tempo di permanenza degli utenti costituiva un indicatore centrale per valutare il successo delle piattaforme. Questa ammissione - presentata come un'evoluzione superata - ha finito per confermare che quelle dinamiche erano note e monitorate, offrendo alla giuria un elemento cruciale. Quando una società afferma di non avere intenzione di causare danni, ma emergono documenti che mostrano la consapevolezza dei rischi, si tratta di stabilire se il danno sia stato considerato e accettato come conseguenza possibile di scelte progettuali orientate ad altri obiettivi.

YouTube come piattaforma social: una qualificazione che pesa
Google ha cercato di posizionare YouTube come un servizio assimilabile alla televisione, sottraendolo alle logiche del contenzioso sui social media. La giuria ha invece accettato l'impostazione opposta, riconoscendo che anche YouTube presenta caratteristiche tipiche delle piattaforme social: il ruolo centrale degli algoritmi nella selezione dei contenuti e la capacità di costruire percorsi di fruizione personalizzati e potenzialmente senza interruzioni. Una qualificazione non tecnica ma giuridica, che apre YouTube a obblighi e responsabilità finora riservati ai social network.

Le implicazioni: oltre 3.000 cause pendenti
Il verdetto di Los Angeles si inserisce in un contesto in cui oltre 3.000 cause simili sono già pendenti in California ed è considerato un caso pilota: non crea un precedente vincolante, ma offre indicazioni concrete su come le giurie possono valutare queste controversie. I danni punitivi riconosciuti - il cui ammontare sarà stabilito in una seduta successiva - hanno una funzione segnaletica più che risarcitoria: indicano che la giuria ha ritenuto il comportamento delle aziende non solo dannoso, ma meritevole di una risposta che vada oltre il ristoro della vittima.

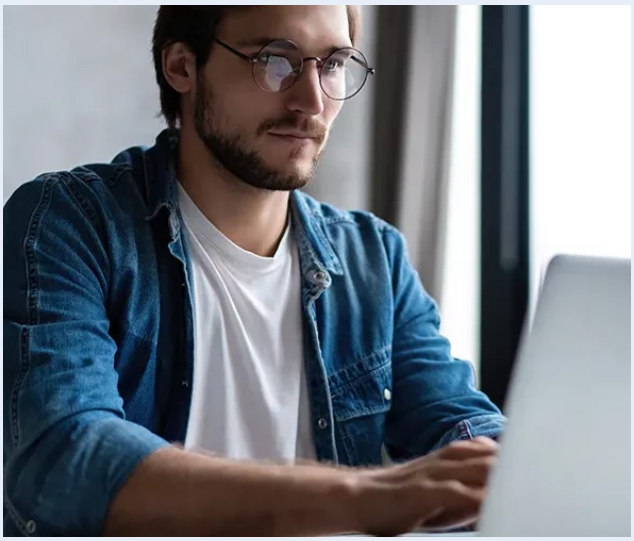
Conclusioni
Entrambi i verdetti convergono su un principio che le piattaforme non potranno più ignorare: la responsabilità non nasce solo da ciò che gli utenti fanno sulle piattaforme, ma da come quelle piattaforme sono state progettate. In Europa, dove il Digital Services Act impone già obblighi specifici di tutela dei minori e valutazione dei rischi algoritmici per le piattaforme di grandi dimensioni, questi verdetti americani offriranno ai regolatori argomenti concreti per chiedere conto delle scelte di design. Il vero costo dei 375 milioni e dei 3 milioni non è finanziario. È il precedente.

Allinea
Avvera Compliance Review
Aprile 2026

Smart working e sicurezza: dal 7 aprile 2026 l'informativa diventa sanzionabile.

La guida operativa per i datori di lavoro

Dal 7 aprile 2026 è in vigore la "legge annuale per le PMI" (legge n. 34/2026, G.U. n. 68 del 23 marzo 2026). L'articolo 11 inserisce il nuovo comma 7-bis nell'articolo 3 del D.Lgs. 81/2008 e modifica l'articolo 55, estendendo l'apparato sanzionatorio del Testo Unico sulla Sicurezza agli obblighi di informativa nel lavoro agile. Non è una riforma epocale, ma ha un effetto immediato e concreto: un obbligo che esisteva già diventa per la prima volta direttamente sanzionabile dagli organi di vigilanza. Per i datori di lavoro che non si sono ancora adeguati, il margine per farlo senza conseguenze si è esaurito ieri.



La novità vera: non un nuovo obbligo, ma un nuovo rischio
L'obbligo di consegnare un'informativa scritta annuale ai lavoratori in smart working era già scritto nell'articolo 22 della legge n. 81/2017. Ciò che mancava era la conseguenza. Fino al 6 aprile 2026, il datore di lavoro inadempiente esponeva se stesso a una responsabilità civile in caso di infortunio, ma non era esposto a sanzioni azionabili in via amministrativa o penale dall'Ispettorato del Lavoro. Dal 7 aprile quella lacuna è colmata. La violazione è ora sanzionata con l'arresto da due a quattro mesi oppure con un'ammenda da 1.708,61 a 7.403,96 euro - importi rivalutati ai sensi del D.D. INL n. 111/2023, sanzioni alternative tra loro. Nella prassi ispettiva, l'INL emette tipicamente una prescrizione obbligatoria prima di procedere ulteriormente; ma il presupposto perché scatti è già integrato dalla semplice mancata consegna. La norma si applica a tutti i datori di lavoro, indipendentemente dalle dimensioni: non è una misura riservata alle PMI nonostante la legge che la contiene.

" L'errore più comune è ridurre l'informativa a una nota sull'ergonomia della postazione"

Cosa deve contenere l'informativa: il perimetro è più ampio di quanto si pensi
L'errore più comune è ridurre l'informativa a una nota sull'ergonomia della postazione. Il perimetro normativo è più esteso: il documento, che deve essere consegnato con cadenza al meno annuale, deve coprire i rischi generali e specifici dell'attività svolta fuori dai locali aziendali, il che include rischi ergonomici (postazione fissa, portatili, tablet), rischio elettrico, illuminazione, qualità dell'aria, microclima, sicurezza antincendio e, per chi lavora in mobilità, rischi outdoor. Devono essere inclusi anche i rischi psico-sociali: stress lavoro-correlato, isolamento relazionale e disconnessione. Sono rischi specifici del lavoro agile riconosciuti dall'INAIL; la loro assenza dall'informativa può essere eccepita in sede ispettiva. Un elemento che molti trascurano: l'informativa deve recare la firma datata del lavoratore e del Rappresentante dei Lavoratori per la Sicurezza (RLS). Senza quella firma, il datore di lavoro non ha prova documentale dell'adempimento. In caso di ispezione o di infortunio, un documento privo di sottoscrizione non protegge nessuno.

La guida operativa: cinque passi nell'ordine giusto
Primo: mappare quanti dipendenti sono in smart working, con quale accordo individuale scritto, da quando. L'accordo è un prerequisito - non si può fare smart working senza - e deve essere comunicato al Ministero del Lavoro tramite la procedura telematica dedicata. Chi non ha ancora adempiuto a questa comunicazione è già irregolare, indipendentemente dalla nuova norma.

Smart working e sicurezza: dal 7 aprile 2026 l'informativa diventa sanzionabile.

La guida operativa per i datori di lavoro

Secondo: verificare se tra i lavoratori agili vi siano videoterminalisti ai sensi del D.Lgs. 81/2008 e chi usa il videoterminale sistematicamente per più di 20 ore settimanali. Per questa categoria scattano obblighi aggiuntivi di sorveglianza sanitaria e visite oculistiche periodiche che molte aziende ignorano.

Terzo: redigere o aggiornare l'informativa, verificando che copra tutti i rischi rilevanti e che rechi spazio per le firme datate. Chi l'ha già consegnata più di un anno fa deve rinnovarla: la cadenza annuale non è una raccomandazione, è un requisito di legge.
Quarto: aggiornare il DVR in coerenza con le modalità di lavoro agile adottate.
Quinto: istituire un sistema interno (anche solo un calendario condiviso) che garantisca il rinnovo annuale dell'informativa per ciascun lavoratore agile.

Il quadro d'insieme

Secondo l'ultimo report dell'Osservatorio Smart Working del Politecnico di Milano, in Italia ci sono 3,57 milioni di smart worker. Dietro ciascuno di loro c'è un datore di lavoro che, dal 7 aprile, risponde penalmente e amministrativamente se non ha consegnato l'informativa. La norma non distingue tra chi non sapeva e chi ha scelto di non adeguarsi: l'inadempimento è oggettivo. Chi è ancora fermo può rimediare subito, ma ogni giorno che passa è un giorno di esposizione inutile.

Allinea
Avvera Compliance Review
Aprile 2026

Allucinazioni da AI in aula: il Tribunale di Siracusa fissa il principio.

L'uso acritico dell'intelligenza artificiale è colpa grave

Con la sentenza n. 338 del 20 febbraio 2026, il Tribunale di Siracusa ha inflitto a un avvocato del Foro di Milano una sanzione complessiva di circa 30.000 euro per aver fondato la propria difesa su quattro precedenti della Cassazione che, a una verifica nel CED della Suprema Corte, si sono rivelati inutilizzabili: le sentenze esistevano, ma trattavano materie del tutto estranee alla causa. Le massime virgolettate riportate negli atti erano state generate ex novo da un sistema di intelligenza artificiale generativa. Non si trattava di un refuso. Era il risultato di una delega in bianco a uno strumento che non sa distinguere tra ciò che è vero e ciò che è plausibile.

I fatti

La vicenda riguarda un contenzioso civile su un contratto di sublocazione immobiliare. A sostegno delle proprie tesi, il difensore ha inserito nella memoria quattro richiami alla giurisprudenza di legittimità, completi di estratti testuali virgolettati. Il giudice, insospettito dalla formulazione delle massime, ha effettuato una verifica diretta nel database della Cassazione: nessuno dei quattro riferimenti conteneva i passaggi riportati. Le sentenze - Cass. n. 1216/2000, n. 8379/2006, n. 14795/2003 e n. 4553/2004 - erano reali, ma i contenuti attribuiti loro dall'AI non lo erano. Una consultazione elementare delle fonti primarie avrebbe smascherato l'errore in pochi minuti.

Allucinazioni da AI in aula: il Tribunale di Siracusa fissa il principio.

L'uso acritico dell'intelligenza artificiale è colpa grave

Il principio: uso acritico dell'AI è colpa grave

Il giudice ha chiarito che i modelli linguistici di grandi dimensioni non sono banche dati giuridiche: non recuperano informazioni, ma producono testo statisticamente coerente con il contesto in cui operano. Chi si avvale di uno strumento del genere per redigere atti giudiziari senza verificare sistematicamente ogni output sulle fonti primarie non commette un errore scusabile, ma una negligenza qualificata. Allo stato attuale delle conoscenze tecnologiche, sostenere di non sapere che un LLM possa inventare sentenze non è più una difesa credibile - e il giudice lo ha detto esplicitamente. La sanzione si articola su tre voci: oltre 14.000 euro di spese legali alla controparte, un importo equivalente a titolo di responsabilità aggravata ex art. 96, comma 3, c.p.c., e 2.000 euro alla Cassa delle Ammende per il danno arrecato all'amministrazione della giustizia.

Una giurisprudenza italiana in costruzione

Siracusa non è un caso isolato, è l'ultimo stadio di un orientamento che si sta consolidando con una coerenza difficile da ignorare. Il Tribunale di Torino aveva aperto la serie il 16 settembre 2025, censurando atti difensivi costruiti con il supporto dell'AI e caratterizzati da citazioni giurisprudenziali inconferenti prive di qualsiasi filo logico rispetto al caso concreto. Il Tribunale di Latina aveva replicato una settimana dopo, con due pronunce gemelle del 23 settembre 2025, sanzionando un difensore che aveva prodotto centinaia di ricorsi seriali evidentemente generati in modo automatizzato. Tre tribunali, quattro sentenze, un principio che converge: l'uso acritico dell'AI generativa nella redazione di atti giudiziari integra responsabilità processuale aggravata.

Il quadro normativo nel frattempo si è definito. Il Regolamento UE 2024/1689 e la legge italiana n. 132/2025 che ne ha disposto il recepimento introducono obblighi specifici per i professionisti intellettuali che utilizzano sistemi di intelligenza artificiale, tra cui l'obbligo di informare il cliente dell'impiego di tali strumenti. Una norma che, letta insieme alla giurisprudenza in esame, delinea un regime di responsabilità professionale sempre più preciso - e sempre meno eludibile.

" Un sistema integrato con banche dati certificate può supportare la ricerca giurisprudenziale "

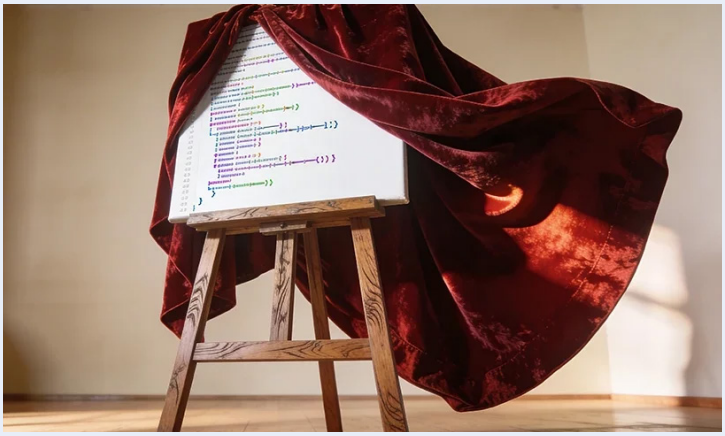
Le implicazioni per la professione forense

L'uso dell'AI nella pratica legale non è il problema. Lo è la confusione tra due funzioni radicalmente diverse: il recupero di informazione verificata e la generazione di testo plausibile. Un sistema integrato con banche dati certificate può supportare la ricerca giurisprudenziale, l'analisi documentale, la strutturazione di argomenti difensivi. Un LLM generalista non fa nulla di tutto questo - produce sequenze linguistiche coerenti con il contesto, indipendentemente dalla loro corrispondenza alla realtà. La firma in calce a un atto giudiziario non attesta solo la paternità del testo. Certifica che chi lo ha redatto si è assunto la responsabilità del suo contenuto - in fatto, in diritto, nelle citazioni. Quella responsabilità non si trasferisce allo strumento. La sentenza di Siracusa, insieme ai precedenti di Torino e Latina, sta traducendo in sanzioni concrete un principio che l'AI Act e la legge 132/2025 avevano già codificato: la supervisione umana sull'uso dell'intelligenza artificiale non è una raccomandazione. È un obbligo. E i tribunali italiani hanno iniziato a farlo rispettare.

Allinea
Avvera Compliance Review
Aprile 2026

Il codice di Claude esposto per errore: un incidente che vale molto più di un leak

Il 31 marzo 2026 Anthropic ha accidentalmente pubblicato il codice sorgente completo della sua CLI Claude Code all'interno di un pacchetto npm pubblico, rendendo accessibili circa 512.000 righe di TypeScript. L'azienda ha confermato l'incidente attribuendolo a un errore umano nel processo di packaging del rilascio: la versione 2.1.88 di Claude Code è stata distribuita con un file source map da 59,8 MB che puntava direttamente a un archivio zip accessibile sul bucket Cloudflare R2 di Anthropic. Nessuno ha dovuto hackerare nulla. Il file era semplicemente lì. Non si trattava di un attacco, né di una violazione di sicurezza nel senso tecnico del termine. Eppure il caso merita attenzione ben oltre la cronaca tecnologica.



Cosa conteneva il codice e cosa è successo dopo
Il codice trapelato comprende circa 1.900 file TypeScript, tra cui moduli chiave come il Query Engine responsabile della gestione delle chiamate ai modelli. Tra le funzionalità interne emerse figura un sistema di orchestrazione multi-agente che consente a Claude Code di generare sciami di agenti paralleli per gestire task complessi, un IDE Bridge che collega il terminale alle estensioni per editor come VS Code e JetBrains, e funzionalità non documentate come la modalità Undercover - che istruisce il sistema a evitare riferimenti ad Anthropic nei commit pubblici - e un modulo denominato KAIROS, progettato per consentire al tool di operare in background come agente persistente.

Prima che Anthropic potesse intervenire, il materiale era già stato copiato su GitHub, dove il repository ha collezionato più di 50.000 fork nel giro di pochissime ore. Alcuni mirror sono stati usati per distribuire malware come Vidar e GhostSocks. La presenza di logiche di hook e dei permessi ha fornito ai malintenzionati materiale per individuare vulnerabilità note, tra cui il CVE-2025-59536 e il CVE-2026-21852, che possono consentire potenziali attacchi RCE attraverso configurazioni particolari.

Non è la prima volta - ed è il secondo incidente in una settimana
Questa è la seconda volta che si verifica lo stesso errore: una fuga di source map quasi identica si era verificata con una versione precedente di Claude Code nel febbraio 2025. E cinque giorni prima, il 26 marzo, un errore di configurazione del CMS aveva esposto circa 3.000 file interni contenenti dettagli sul modello inedito Claude Mythos, anch'esso attribuito a un errore umano. Due incidenti quasi identici in tredici mesi, e un terzo nello spazio di una settimana. Il pattern conta più del singolo episodio.

I profili giuridici rilevanti
Il caso apre almeno tre questioni distinte. La prima riguarda la proprietà intellettuale. Parte del codice sorgente finito online è protetto da diritto d'autore, e il fatto che sia stato accessibile potrebbe consentire ai concorrenti di Anthropic di osservare più da vicino le potenzialità del software e capire meglio come funziona la sua architettura. Chi ha scaricato e utilizza quel codice per sviluppare prodotti concorrenti si espone a responsabilità per violazione di diritto d'autore, indipendentemente dal fatto che il rilascio sia stato involontario. La seconda questione riguarda la supply chain software. Un file .npmignore configurato male e un bucket pubblico Cloudflare hanno reso accessibile l'architettura interna di uno dei modelli AI più diffusi al mondo.

Il codice di Claude esposto per errore: un incidente che vale molto più di un leak

Per le organizzazioni che integrano Claude Code nei propri workflow di sviluppo, il caso pone un tema di sicurezza della catena di fornitura che non può essere liquidato come problema di Anthropic: chi usa componenti di terze parti nei propri sistemi eredita anche i rischi di una governance insufficiente sui processi di rilascio del fornitore. La terza questione riguarda la reputazione e le conseguenze regolamentari. Tutto questo accade mentre Anthropic si starebbe preparando alla quotazione in borsa, un'operazione che richiede fiducia, solidità e una reputazione impeccabile. In un contesto in cui l'AI Act europeo impone obblighi di documentazione tecnica e trasparenza sui sistemi ad alto rischio, incidenti ripetuti di questo tipo alimentano dubbi sulla maturità dei processi interni di un'azienda che ha costruito il proprio posizionamento proprio sulla sicurezza dell'intelligenza artificiale.

" chi usa componenti di terze parti nei propri sistemi eredita anche i rischi di una governance insufficiente sui processi di rilascio del fornitore "

Conclusioni

La dichiarazione di Anthropic - errore umano, nessun dato compromesso, misure correttive in corso - è tecnicamente corretta. Ma la distinzione tra errore operativo e breach, per quanto legittima sul piano tecnico, non riduce la rilevanza del caso. Un processo di build che per la seconda volta in tredici mesi include in produzione artefatti di debug contenenti codice proprietario non è un problema di singolo individuo. È un problema di governance. E per un'azienda che aspira a definire gli standard di sicurezza dell'intelligenza artificiale, è esattamente il tipo di problema che non dovrebbe verificarsi una volta, figurarsi due.

Allinea
Avvera Compliance Review
Aprile 2026

Microsoft Copilot e il flex routing: un opt-out che non avrebbe dovuto esistere

Microsoft 365 Copilot è lo strumento di intelligenza artificiale più adottato negli ambienti aziendali europei. Integrato nell'ecosistema M365, accede in tempo reale a email, documenti, conversazioni Teams e dati di calendario tramite Microsoft Graph. Il 7 aprile 2026, mentre le organizzazioni europee erano impegnate a valutarne la compliance, Microsoft ha annunciato l'introduzione del flex routing - una funzionalità che consente di instradare l'elaborazione dei prompt al di fuori dell'Unione Europea durante i picchi di utilizzo. E lo ha fatto attivandola per impostazione predefinita.

Cosa prevede il flex routing

La comunicazione è arrivata tramite il post MC1269223 del Message Center di Microsoft. A partire dal 17 aprile 2026, il flex routing sarebbe stato abilitato automaticamente per tutti i tenant europei idonei - con onere per gli amministratori di disabilitarlo attivamente se non lo ritenevano appropriato. Per i tenant creati dopo il 25 marzo 2026, la funzionalità sarebbe stata abilitata direttamente alla creazione. In altri termini: un sistema opt-out. Il meccanismo è tecnicamente descritto da Microsoft come sicuro. I dati restano cifrati in transito e a riposo, i dati a riposo rimangono in territorio europeo, e i dati trasferiti fuori dall'UE per esigenze operative vengono pseudonimizzati. Ma la sicurezza tecnica non esaurisce la questione giuridica.
Nel momento dell'inferenza - cioè quando Copilot elabora un prompt - il trattamento avviene fuori dall'Unione Europea. E quel prompt include non solo la richiesta dell'utente, ma anche i dati aziendali e i file condivisi necessari a generare la risposta.

Microsoft Copilot e il flex routing: un opt-out che non avrebbe dovuto esistere

La frizione con il GDPR

Il GDPR non si limita a disciplinare dove i dati sono conservati. Regola ogni operazione di trattamento, inclusa l'elaborazione temporanea. Un trasferimento verso paesi terzi - anche se limitato alla fase di inferenza - richiede una base giuridica adeguata ai sensi degli articoli 44 e seguenti del Regolamento. Un sistema opt-out significa che le organizzazioni che non avessero rilevato la comunicazione nel Message Center si sarebbero ritrovate a trasferire dati fuori dall'UE senza averlo valutato e senza una base giuridica consapevolmente identificata. Non è un'ipotesi teorica: è la realtà operativa della maggior parte delle organizzazioni, dove il Message Center non viene monitorato sistematicamente da chi è responsabile della gestione privacy. Il principio di privacy by design, sancito dall'art. 25 del GDPR, impone che le impostazioni predefinite dei sistemi che trattano dati personali garantiscano il livello più elevato di protezione. Un default che sposta il trattamento fuori dall'EU senza una valutazione consapevole del titolare va nella direzione opposta - e non è sanabile dal fatto che la funzionalità sia tecnicamente sicura o che Microsoft la documenti in modo trasparente. Trasparenza e conformità non sono la stessa cosa.

Le implicazioni per i vostri sistemi

Per le organizzazioni che hanno adottato Copilot a seguito della formazione che abbiamo condotto insieme, la vicenda ha due implicazioni operative dirette.

La prima: le impostazioni predefinite di M365 e Copilot non sono statiche. Cambiano nel tempo tramite comunicazioni di servizio che non sempre raggiungono chi è responsabile della gestione privacy. Il monitoraggio del Message Center non è un'attività discrezionale - è un presidio necessario per mantenere la conformità nel tempo. Ogni modifica rilevante va valutata congiuntamente dall'amministratore IT, dal DPO e dal titolare del trattamento prima che entri in vigore. La seconda: la responsabilità della compliance rimane in capo al titolare. Microsoft può cambiare le impostazioni predefinite dei propri servizi - e lo fa. Delegare la verifica di queste modifiche al solo reparto IT, senza un processo strutturato di governance, espone l'organizzazione a rischi che non dipendono da negligenza ma da una catena di responsabilità non presidiata.

Aggiornamento

Secondo quanto riportato da ITdaily, che cita una conferma diretta di Microsoft alla redazione olandese di Tweakers, Microsoft ha parzialmente invertito la propria posizione: il flex routing per i tenant europei passerà da sistema opt-out a sistema opt-in. Per impostazione predefinita, i dati degli utenti europei resteranno elaborati in territorio UE. La correzione è positiva - ma arriva dopo che il problema era già stato sollevato pubblicamente. Il punto rimane: un opt-out di questo tipo non avrebbe dovuto essere progettato.

Allinea
Avvera Compliance Review
Aprile 2026

United States v. Heppner: quando l'AI cancella il segreto professionale

Il caso in sintesi

Il 17 febbraio 2026 il giudice Jed S. Rakoff del Southern District of New York ha depositato la propria opinione scritta in United States v. Heppner, dopo aver già pronunciato il dispositivo il 10 febbraio. Si tratta della prima decisione federale americana ad affrontare la questione se le conversazioni di un imputato con uno strumento di intelligenza artificiale generativa siano protette dal privilegio avvocato-cliente o dalla work product doctrine.

Bradley Heppner, dirigente finanziario di Dallas, era stato indagato e poi rinviato a giudizio per frode sui mercati finanziari e wire fraud. Dopo aver ricevuto una citazione del grand jury e aver ingaggiato un avvocato difensore, ma prima del proprio arresto, Heppner aveva usato di propria iniziativa - senza direzione del legale - la versione consumer di Claude, lo strumento AI sviluppato da Anthropic, per elaborare la propria strategia difensiva, analizzare la propria esposizione penale e preparare documenti da condividere con i propri avvocati. L'FBI, nel corso della perquisizione domiciliare seguita all'arresto, aveva sequestrato 31 documenti contenenti questi scambi con Claude. La difesa aveva invocato il privilegio. Il governo aveva chiesto al giudice di dichiarare che quei documenti non erano protetti. Il giudice Rakoff ha accolto la richiesta del governo su tutti i punti.

Le tre ragioni del rigetto

Il giudice Rakoff ha identificato almeno due ragioni autonomamente sufficienti per negare il privilegio, a prescindere da ogni altra considerazione.

Prima: Claude non è un avvocato. Il privilegio avvocato-cliente protegge le comunicazioni tra un cliente e il proprio legale. Un sistema AI non è un avvocato, non ha un rapporto fiduciario con l'utente, non è iscritto a un albo e non è soggetto a deontologia professionale. Nessuna formulazione contrattuale può alterare questo dato strutturale.

Seconda: nessuna ragionevole aspettativa di riservatezza. I termini di servizio consumer di Anthropic - come quelli di tutti i principali provider - riservano il diritto di accedere ai prompt per finalità di training e di divulgarli alle autorità in risposta a richieste legali. Inserire informazioni riservate in un sistema con queste condizioni equivale, secondo il giudice, a discutere la propria strategia difensiva in un luogo pubblico.

Terza - la più insidiosa: la waiver. Heppner aveva inserito in Claude informazioni ricevute dal proprio avvocato difensore. Il giudice ha concordato con il governo che condividere comunicazioni privilegiate con una piattaforma AI terza può costituire rinuncia al privilegio sulle comunicazioni originarie con il legale. Traduzione pratica: non solo i documenti AI erano acquisibili dalla pubblica accusa. Potenzialmente anche le comunicazioni con l'avvocato da cui quelle informazioni provenivano.

Cosa cambia per gli avvocati

La sentenza Heppner introduce un obbligo di informativa che molti avvocati non hanno ancora formalizzato: il dovere di avvertire esplicitamente i propri clienti che qualsiasi informazione immessa in uno strumento AI consumer-grade è potenzialmente scopribile in sede di discovery e non è coperta dal segreto professionale. Questo avvertimento dovrebbe entrare nelle lettere di incarico e nei documenti di onboarding del cliente.

United States v. Heppner: quando l'AI cancella il segreto professionale

Il giudice Rakoff ha peraltro suggerito che il privilegio potrebbe resistere laddove l'uso dell'AI sia diretto dall'avvocato e condotto su piattaforme enterprise con garanzie contrattuali adeguate - a condizione che i termini di servizio escludano l'accesso ai dati per finalità di training e la loro divulgazione a terzi senza consenso. La distinzione tra versione consumer e versione enterprise dello stesso strumento diventa quindi giuridicamente rilevante.

Cosa cambia per le aziende

Il problema non riguarda solo gli avvocati esterni. Il legal counsel interno che usa ChatGPT, Claude o Gemini in versione consumer per analizzare una questione legale, elaborare una strategia o preparare una comunicazione riservata sta potenzialmente creando materiale discoverable in un futuro contenzioso. Le policy aziendali sull'uso dell'AI devono coprire esplicitamente questo scenario, distinguendo tra strumenti autorizzati con adeguate garanzie contrattuali e strumenti consumer non idonei al trattamento di informazioni riservate. Vi è inoltre un profilo che la sentenza non affronta direttamente ma che rileva in modo autonomo: il segreto industriale. Secondo il D.Lgs. 63/2018 (di attuazione della direttiva Trade Secrets), la tutela del know-how riservato presuppone che il titolare abbia adottato misure ragionevoli per mantenerlo tale. Un'azienda che consente ai propri dipendenti di immettere informazioni strategiche in strumenti consumer senza policy adeguate non sta adottando alcuna misura - e quella tutela, in caso di contenzioso, rischia di non reggere.

La prospettiva europea

" Il GDPR impone che i dati personali siano trattati in modo da garantirne la riservatezza "

La sentenza Heppner è americana. Ma il principio sottostante - che condividere informazioni riservate con un provider AI terzo può costituire divulgazione non autorizzata - è pienamente compatibile con il quadro normativo europeo. Il GDPR impone che i dati personali siano trattati in modo da garantirne la riservatezza; i trasferimenti a provider extra-UE richiedono garanzie adeguate; gli avvocati italiani ed europei sono soggetti a obblighi deontologici di riservatezza che non si esauriscono con il rispetto della legge americana. Chi opera esclusivamente in Europa e ritiene che il problema non lo riguardi si sbaglia. La questione non è di giurisdizione - è di principio. E il principio è lo stesso: ciò che viene condiviso con una piattaforma AI consumer non è riservato.

Allinea
Avvera Compliance Review
Aprile 2026

NIS2 e le nuove determinazioni ACN: cosa devono fare adesso le imprese

Il 13 aprile 2026 l'Agenzia per la Cybersicurezza Nazionale ha adottato due Determinazioni (127434/2026 e 127437/2026) in aggiornamento al quadro attuativo del decreto legislativo n. 138/2024, con cui l'Italia ha recepito la Direttiva NIS2. Le due Determinazioni introducono ulteriori adempimenti da gestire mediante il portale ACN e avviano un processo di categorizzazione che cambierà il modo in cui i soggetti NIS documentano le proprie attività critiche. Per le imprese già registrate o prossime all'iscrizione, il tempo per adeguarsi è definito e non comprimibile.

I nuovi soggetti NIS 2026: le scadenze operative

La Determinazione 127434/2026, in vigore dal 30 aprile 2026, riguarda i soggetti inseriti per la prima volta nell'elenco NIS nel corso del 2026. Per questi, il quadro delle

NIS2 e le nuove determinazioni ACN: cosa devono fare adesso le imprese

scadenze è il seguente: le misure di sicurezza previste dagli allegati alla Determinazione del 19 dicembre 2025 dovranno essere adottate entro il 31 luglio 2027; l'obbligo di notifica degli incidenti significativi decorre dal 1° gennaio 2027; gli eventuali obblighi specifici in materia di sicurezza e resilienza dei sistemi di nomi di dominio seguono anch'essi la scadenza del 31 luglio 2027. La scelta di concedere un periodo di adeguamento fino al 2027 riflette la consapevolezza che costruire un sistema di gestione della cybersicurezza conforme alla NIS2 non è un adempimento documentale, ma un investimento organizzativo che richiede tempo, risorse e revisione dei processi interni. Non è, però, un lasciapassare per l'inerzia: il percorso va avviato adesso.

La novità strutturale: la categorizzazione delle attività e dei servizi

La Determinazione 127437/2026 - in vigore dal 15 aprile 2026, con il Capo V sulla categorizzazione che scatta dal 1° maggio - predispone le modifiche al portale ACN per quello che è probabilmente l'obbligo più rilevante dal punto di vista operativo: ogni anno, dal 1° maggio al 30 giugno, i soggetti NIS dovranno comunicare tramite il nuovo Servizio NIS/Categorizzazione l'elenco categorizzato delle proprie attività e servizi, attribuendo a ciascuno le categorie di rilevanza stabilite dall'ACN. Il meccanismo è chiaro: l'ACN vuole una mappatura strutturata delle funzioni critiche dei soggetti NIS, e si aspetta che venga prodotta con puntualità e precisione.

" l'ACN vuole una mappatura strutturata delle funzioni critiche dei soggetti NIS "

I fornitori rilevanti: un nuovo censimento obbligatorio

La stessa Determinazione introduce la struttura che nel portale ACN consentirà di adempiere all'obbligo di censire i fornitori rilevanti NIS: i soggetti che forniscono prodotti o servizi ICT al soggetto NIS, oppure la cui interruzione avrebbe un impatto significativo sulla continuità operativa. Per ciascun fornitore rilevante dovranno essere indicati denominazione, codice fiscale, paese di sede legale, codici CPV relativi alle forniture e il criterio di rilevanza applicato. Si tratta di un obbligo che impone una revisione della catena di approvvigionamento con occhi diversi rispetto al passato: non più solo contrattuale o commerciale, ma sistemica e orientata al rischio cyber. Le imprese che non hanno mai mappato le proprie dipendenze critiche da fornitori tecnologici dovranno farlo entro il prossimo aggiornamento annuale.

Le altre modifiche operative

La Determinazione prevede inoltre che, in caso di indisponibilità del referente CSIRT e dei suoi sostituti, il punto di contatto possa effettuare le notifiche di incidenti in via eccezionale. Per le entità finanziarie soggette al Regolamento DORA, sono previste esenzioni dall'obbligo di designazione del referente CSIRT e dal processo di categorizzazione, con facoltà di adesione volontaria. Per i soggetti già registrati nell'elenco NIS 2025, la piattaforma presenterà informazioni precompilate all'avvio dell'aggiornamento annuale 2026, sulla base di quanto trasmesso fino al 14 aprile 2026. Un alleggerimento procedurale apprezzabile, che non riduce però la responsabilità del soggetto sulla correttezza e completezza dei dati confermati.

Allinea
Avvera Compliance Review
Aprile 2026

Il modello DPIA dell'EDPB: uno strumento utile o un benchmark implicito?

Il 20 aprile 2026 l'EDPB ha aperto una consultazione pubblica su un modello di valutazione d'impatto sulla protezione dei dati - la DPIA prevista dall'art. 35 del GDPR. La consultazione resterà aperta fino al 9 giugno 2026, al termine della quale l'EDPB licenzierà un modello definitivo che ciascuna autorità di controllo nazionale potrà adottare come documento unico o come riferimento per i propri modelli specifici.
Il modello proposto è una tabella in formato Word, strutturata in coerenza con l'art. 35 del GDPR e con le linee guida WP248 già in vigore. Non modifica i criteri esistenti e il documento guida che l'accompagna - l'EDPB DPIA Template explainer - consente alle organizzazioni di condurre la valutazione in modo dettagliato, con indicazioni metodologiche sulla valutazione dei rischi. La domanda rilevante non è cosa contiene il modello, ma cosa diventerà.

"la DPIA è un processo di ragionamento che il titolare compie prima di avviare un trattamento"

Il problema del benchmark implicito
Fino ad oggi, le linee guida WP248 non prevedevano un modello comune di riferimento. La scelta è rimessa ai titolari, in forza del principio di accountability, a condizione che ne rispettassero gli elementi costitutivi. Il modello proposto dall'EDPB non cambia formalmente questa impostazione. Se una o più autorità di controllo nazionali decidessero di veicolare la richiesta di consultazione preventiva, secondo il meccanismo previsto dall'art. 36 GDPR quando la DPIA indica un rischio elevato residuo, attraverso una DPIA redatta secondo il modello EDPB, o se nei propri interventi correttivi adottassero quel modello come standard di riferimento implicito, l'effetto pratico sarebbe quello di trasformare uno strumento facoltativo in un benchmark de facto. Le organizzazioni si troverebbero a dover giustificare le proprie scelte di metodo non più rispetto alla norma, ma rispetto a un formato specifico che non hanno adottato.

Le criticità del modello
Il formato one size fits all mal si concilia con la varietà dei trattamenti che possono richiedere una DPIA. Un sistema di videosorveglianza in un condominio, una piattaforma di profilazione per finalità commerciali e un sistema di intelligenza artificiale applicato alle decisioni in materia di credito hanno poco in comune, eppure tutti e tre potrebbero richiedere una valutazione d'impatto. Un modello generico, per quanto ben strutturato, non cattura questa eterogeneità.

Il punto che conta davvero
Al di là della forma, il modello contiene un messaggio che vale più della tabella stessa: la DPIA non è un adempimento burocratico. È un processo di ragionamento che il titolare compie prima di avviare un trattamento, documentando le proprie scelte in modo coerente e motivato - licità, necessità, proporzionalità, sicurezza. Ogni passaggio è l'occasione di assumere consapevolmente una responsabilità, non di compilare un campo. Chi oggi gestisce la DPIA come una formalità da sbrigare prima dell'avvio di un progetto si espone a un rischio che non dipende dal formato scelto, ma dalla qualità del ragionamento che vi sta dietro. Il modello EDPB, con tutti i suoi limiti, questo lo ricorda.

Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Aprile

AVVERA | SB Società Benefit

Largo Umberto Boccioni 1
21040 Origgio VA
T. +39 02 96515401

Altre sedi
Milano - Pesaro - Udine

avvera.it - info@avvera.it