Supply chain e NIS

Allinea

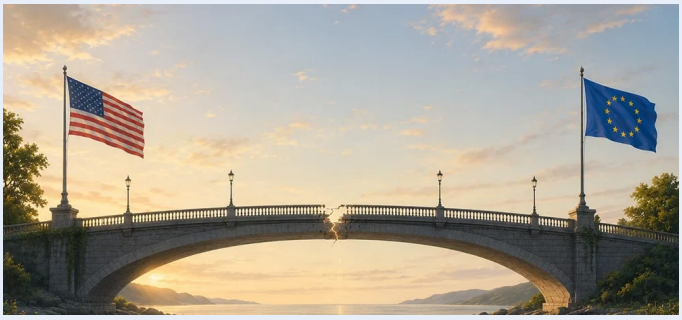
Avvera Compliance Review

Luglio 2026

Allinea
Avvera Compliance Review
Luglio 2026

Data Privacy Framework a rischio?

La recente decisione della Corte Suprema degli Stati Uniti nel caso Trump v. Slaughter potrebbe avere effetti ben più ampi della sola ridefinizione dei rapporti tra Presidente e autorità amministrative indipendenti. La pronuncia, infatti, ha immediatamente acceso il dibattito anche in Europa, dove Max Schrems e l'associazione noyb hanno sostenuto che essa incida direttamente sulla tenuta del EU-US Data Privacy Framework (DPF), il meccanismo che dal 2023 consente il trasferimento di dati personali dall'Unione europea agli Stati Uniti sulla base della decisione di adeguatezza adottata dalla Commissione europea. Sebbene sia prematuro parlare di una nuova invalidazione del quadro normativo e un ipotetico "Schrems III", la questione merita attenzione, soprattutto per le imprese che fanno affidamento quotidianamente sul Data Privacy Framework per i propri flussi transatlantici di dati.



Perché questa sentenza interessa il GDPR?
Il collegamento tra la pronuncia americana e il diritto europeo non è immediato, ma è giuridicamente significativo. La sentenza della Corte Suprema ha infatti superato il precedente Humphrey's Executor v. United States, riconoscendo al Presidente il potere di rimuovere liberamente i commissari della Federal Trade Commission (FTC), fino ad oggi considerata una delle principali autorità amministrative indipendenti degli Stati Uniti. La FTC riveste un ruolo centrale anche nel Data Privacy Framework.

La decisione di adeguatezza della Commissione europea individua infatti tale autorità come uno degli organismi chiamati a garantire l'effettività degli obblighi assunti dalle organizzazioni statunitensi che aderiscono al Framework, nonché l'applicazione delle misure di enforcement nei confronti delle imprese che violano gli impegni assunti. Proprio su questo punto si concentra la lettera inviata da Max Schrems alla Commissione europea. La posizione di Max Schrems: è venuto meno uno dei presupposti del Data Privacy Framework? Secondo noyb, la pronuncia della Corte Suprema avrebbe eliminato uno dei presupposti fondamentali su cui si fonda la decisione di adeguatezza: l'indipendenza della Federal Trade Commission. Se la FTC è oggi pienamente soggetta al potere di revoca del Presidente, essa non potrebbe più essere qualificata come autorità indipendente nel significato richiesto dal diritto dell'Unione europea. L'argomento richiama direttamente l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16 del TFUE, che attribuiscono particolare rilievo all'esistenza di autorità di controllo indipendenti nella tutela dei dati personali. Secondo Schrems, qualora venga meno tale requisito, verrebbe meno anche una delle condizioni che avevano consentito alla Commissione di concludere che gli Stati Uniti assicurano un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione. La richiesta rivolta alla Commissione non è quella di una revoca immediata del Data Privacy Framework, bensì di avviare una rivalutazione della decisione di adeguatezza e, ove necessario, procedere a un ritiro ordinato del provvedimento.

"La richiesta rivolta alla Commissione è quella di avviare una rivalutazione della decisione di adeguatezza e procedere a un ritiro ordinato del provvedimento"

Il Data Privacy Framework è davvero destinato a cadere?
Anzitutto, la sentenza della Corte Suprema riguarda esclusivamente il rapporto costituzionale tra Presidente e commissari della FTC. Essa non modifica né i poteri attribuiti all'autorità né il quadro normativo che disciplina le sue funzioni di enforcement. Rimane quindi aperta la questione se una diversa disciplina della revocabilità dei commissari sia sufficiente, di per sé, a compromettere il livello di tutela richiesto dall'articolo 45 del GDPR. Occorre inoltre ricordare che la decisione di adeguatezza non si fonda esclusivamente sulla FTC. Il Data Privacy Framework è il risultato di un sistema articolato che comprende gli impegni assunti dall'Amministrazione statunitense mediante Executive Order 14086, i nuovi meccanismi di ricorso per gli inte-

Data Privacy Framework a rischio?

ressati europei, le limitazioni alle attività di intelligence e il sistema di certificazione delle imprese aderenti. La valutazione di adeguatezza è quindi complessiva e tiene conto dell'ordinamento statunitense nel suo insieme. Ciò non significa, tuttavia, che la questione possa essere sottovalutata. L'esperienza dei precedenti Schrems I e Schrems II dimostra come gli equilibri dei trasferimenti internazionali possano cambiare rapidamente quando emergono dubbi circa l'effettiva equivalenza delle garanzie offerte dal Paese terzo.

Cosa significa per le imprese?
Per le organizzazioni europee il Data Privacy Framework continua ad essere pienamente efficace e costituisce, allo stato, una valida base giuridica per i trasferimenti verso gli Stati Uniti. Tuttavia, è opportuno monitorare con attenzione l'evoluzione del contesto normativo e giurisprudenziale, predisponendo strategie di compliance che non si fondino esclusivamente sulla decisione di adeguatezza, ma che mantengano disponibili anche strumenti alternativi, quali le Clausole Contrattuali Standard e le valutazioni supplementari richieste dalla giurisprudenza europea. Il dibattito aperto dalla sentenza Trump v. Slaughter conferma ancora una volta come la governance dei dati personali sia ormai profondamente influenzata non solo dal diritto della protezione dei dati, ma anche dalle evoluzioni del diritto costituzionale, del diritto amministrativo e della geopolitica digitale.
Monitorare gli sviluppi, valutare periodicamente le basi giuridiche dei trasferimenti e adottare un modello di compliance dinamico non significa soltanto rispettare il GDPR, ma anche ridurre il rischio operativo e garantire continuità ai processi aziendali in un contesto normativo sempre più complesso e in continua evoluzione.

Allinea
Avvera Compliance Review
Luglio 2026

Cosa insegna alle imprese il caso di un'infrastruttura critica colpita

Il 26 giugno 2026 Trenitalia ha comunicato ai clienti coinvolti un incidente di sicurezza informatica con accesso non autorizzato a dati personali relativi ai titoli di viaggio. La comunicazione è stata effettuata ai sensi dell'art. 34 del GDPR, che impone la comunicazione agli interessati quando la violazione comporta un rischio elevato per i loro diritti e libertà. L'azienda ha notificato l'accaduto al Garante per la protezione dei dati personali e al CSIRT Italia, presentando denuncia alla Procura della Repubblica presso il Tribunale di Roma. La sostanza giuridica del caso, però, merita un'analisi più approfondita. Perché tocca punti che ogni titolare del trattamento dovrebbe avere a mente.

"La comunicazione agli interessati, quando ricorre il rischio elevato, deve avvenire anch'essa senza ritardo"

Il dato di partenza: ottobre 2025, comunicazione giugno 2026
Il primo elemento da segnalare è temporale. Trenitalia ha specificato che l'attacco è avvenuto a ottobre 2025, ma la procedura per risalire agli utenti coinvolti è stata "lunga e complessa". Sono trascorsi circa otto mesi tra l'evento e la comunicazione agli interessati. L'azienda giustifica il ritardo con le attività di analisi forense necessarie a ricostruire con precisione gli accessi impropri e identificare i clienti coinvolti, in conformità con l'art. 34 GDPR e le linee guida EDPB. Il quadro normativo, però, è preciso: la notifica al Garante deve avvenire senza ingiustificato ritardo, e ove possibile entro 72 ore dalla conoscenza della violazione. La comunicazione agli interessati, quando ricorre il rischio elevato, deve avvenire anch'essa senza ritardo. Il tempo necessario all'analisi forense può giustificare differimenti, ma il Garante valuterà caso per caso se gli otto mesi siano stati proporzionati alla complessità accertativa.

Cosa insegna alle imprese il caso di un'infrastruttura critica colpita

I dati coinvolti: niente credenziali, ma molti più rischi di quanto si pensi
Trenitalia dichiara che non risultano coinvolti dati di accesso agli account, credenziali personali o informazioni di pagamento. Il dato è importante, perché esclude i rischi più immediati di compromissione finanziaria. Ma è anche pericolosamente rassicurante. I dati effettivamente sottratti (nome, cognome, data e luogo di nascita, recapiti email e telefonici, tratta del viaggio, data, orario, numero del titolo, eventuale carta fedeltà, datore di lavoro, estremi del documento d'identità) costituiscono un set informativo di altissimo valore per lo spear phishing. La giurisprudenza del Garante è da tempo orientata in questo senso: la sensibilità dei dati va valutata non solo in astratto, ma in relazione al contesto d'uso che ne possono fare gli attaccanti.

Il doppio binario normativo: GDPR e NIS2
Il caso Trenitalia ha una doppia dimensione che merita di essere distinta. Sul fronte della protezione dei dati personali, si applicano gli artt. 33 e 34 GDPR. Sul fronte della sicurezza dei servizi digitali, il trasporto ferroviario rientra tra i settori ad alta criticità previsti dal D.Lgs. 138/2024 di recepimento della NIS2: l'allegato I include gestori dell'infrastruttura e imprese ferroviarie, e l'art. 25 impone ai soggetti essenziali e importanti la notifica al CSIRT Italia degli incidenti significativi, con pre-notifica entro 24 ore e notifica entro 72 ore dalla conoscenza dell'incidente. Trenitalia ha gestito entrambi i binari. Ma il caso evidenzia un tema strutturale: incidenti che coinvolgono dati personali in settori NIS2 attivano contemporaneamente due regimi di compliance, due autorità di vigilanza, due timeline diverse. La gestione integrata di queste comunicazioni (Garante, CSIRT, Procura), interessati richiede procedure documentate che molte organizzazioni ancora non hanno.

Il precedente Almaviva e il rischio supply chain
L'incidente arriva dopo il caso Almaviva del novembre 2025, in cui un threat actor avrebbe rivendicato la pubblicazione di 2,3 terabyte di dati riconducibili anche al Gruppo Ferrovie dello Stato. Il quadro che emerge è quello di una superficie d'attacco estesa che riguarda non solo l'operatore ferroviario, ma l'intera catena dei fornitori tecnologici. Per le imprese che integrano piattaforme di ticketing, CRM, customer care e gestione documentale di terze parti il caso pone una questione di governance della supply chain che la NIS2 disciplina espressamente: l'art. 24 impone la gestione del rischio nella catena di approvvigionamento come obbligo autonomo dei soggetti NIS.

Cosa devono fare le imprese
Tre indicazioni concrete. Primo: rivedere le procedure di incident response per garantire la gestione integrata GDPR-NIS2, con timeline distinte ma coordinate. Secondo: mappare i fornitori critici e verificare i loro standard di sicurezza (l 'incidente di un fornitore può diventare un proprio incidente nel giro di poche ore). Terzo: trattare i dati transazionali e di servizio con la stessa cura riservata a credenziali e pagamenti. Sono spesso più utili agli attaccanti di quanto si creda.

Allinea
Avvera Compliance Review
Luglio 2026

Recensioni false nel turismo e nella ristorazione

Cosa prevedono le linee guida AGCM

Il 30 giugno l'Autorità Garante della Concorrenza e del Mercato ha posto in consultazione pubblica, fino al 15 luglio, lo schema di Linee guida attuative della legge annuale per le PMI n. 34/2026 in materia di recensioni online nel turismo e nella ristorazione. Il testo dà contenuto operativo ai requisiti di liceità già previsti dalla legge, fornendo agli operatori criteri applicativi delle disposizioni del Codice del consumo in materia di recensioni.

Obblighi di verifica e tracciabilità

Le Linee guida richiedono ai professionisti che raccolgono recensioni sui propri prodotti l'adozione di strumenti idonei a verificare l'effettivo acquisto o utilizzo del bene o servizio recensito. Tra le modalità indicate: documentazione fiscale o contabile, numero d'ordine o di prenotazione, invio dell'invito a recensire all'indirizzo email utilizzato per l'acquisto e solo successivamente al completamento dell'ordine.

È inclusa anche l'opzione del QR code abbinato allo scontrino, soluzione richiesta in sede di audizione dalle associazioni dei consumatori. A questo si aggiungono obblighi di tracciabilità dell'autore della recensione e l'adozione di sistemi automatizzati per l'individuazione di pattern fraudolenti – ad esempio un numero anomalo di recensioni provenienti dallo stesso indirizzo IP in un breve intervallo temporale. L'Autorità distingue due categorie di soggetti obbligati: i professionisti che raccolgono recensioni relative alla propria offerta e i soggetti che pubblicano o gestiscono recensioni relative all'offerta di terzi. Su questi ultimi gravano ulteriori obblighi di gestione tempestiva dei reclami e di rimozione dei contenuti illeciti, in una logica assimilabile a quella prevista per gli hosting provider dal Digital Services Act.

Proporzionalità degli obblighi

Le misure sono modulate in base alle dimensioni e al modello di business dell'operatore. Le piattaforme di maggiori dimensioni, per volumi trattati ed esposizione al rischio di frodi, sono tenute a strumenti più sofisticati, che combinano intelligenza artificiale e revisione umana dei contenuti. Il medesimo livello di presidio non è richiesto a una PMI del settore ricettivo o della ristorazione.

Un profilo applicativo non risolto

Le Linee guida non affrontano in modo esplicito l'ipotesi, segnalata dalle associazioni dei consumatori in audizione, in cui acquisto e pubblicazione della recensione avvengano su piattaforme distinte, con account diversi tra loro non riconducibili. In questo scenario, l'unico elemento idoneo a provare la genuinità della recensione resta la documentazione fiscale in possesso del consumatore, mentre manca un meccanismo che colleghi automaticamente l'identità verificata su una piattaforma con quella utilizzata sull'altra.

Doppio livello regolatorio

Le linee guida applicative sono elaborate separatamente da AGCM e AGCOM: alla prima competono i profili sanzionatori, alla seconda la definizione del Codice di condotta cui le piattaforme devono attenersi in presenza di recensioni illecite. Gli operatori del settore dovranno quindi tenere sotto osservazione due fonti regolatorie distinte, potenzialmente non sincronizzate nei tempi di adozione.

Recensioni false nel turismo e nella ristorazione
Cosa prevedono le linee guida AGCM

Obblighi informativi
È inoltre prevista una serie di obblighi di trasparenza verso i consumatori, relativi alle modalità di pubblicazione, gestione, classificazione e moderazione delle recensioni, ai criteri utilizzati per qualificarle come "verificate" o "autentiche" e all'eventuale presenza di incentivi economici offerti dal professionista in cambio della recensione.

Considerazioni conclusive
Le Linee guida forniscono agli operatori indicazioni applicative che la legge n. 34/2026 non conteneva, in particolare sul piano tecnico e organizzativo. Restano invece aperti i profili relativi all'applicabilità delle regole a piattaforme stabilite fuori dal territorio nazionale e al coordinamento con il quadro normativo europeo, in particolare con il Digital Services Act. Il termine del 15 luglio segna la scadenza utile per la presentazione di osservazioni nell'ambito della consultazione pubblica.

Allinea
Avvera Compliance Review

Il caso Grok Build
Quando l'AI copia il tuo codice senza dirtelo

Il 12 luglio 2026 il ricercatore di sicurezza informatica noto con lo pseudonimo di cereblab ha pubblicato l'esito di un'analisi condotta sul traffico di rete generato da Grok Build, l'assistente di programmazione a linea di comando distribuito da xAI. L'indagine ha accertato che, all'attivazione di ogni sessione, lo strumento apre due canali di comunicazione paralleli verso i server della società: il canale destinato all'interazione con il modello, che veicola i dati strettamente necessari all'evasione della richiesta dell'utente, nell'ordine di alcune centinaia di kilobyte e un secondo canale, non menzionato nella documentazione tecnica del prodotto, per il quale l'intero contenuto del repository Git in uso presso lo sviluppatore, comprensivo dell'integrale cronologia dei commit, veniva trasmesso a un bucket Google Cloud denominato "grok-code-session-traces". Il rapporto tra i volumi movimentati dai due canali si è attestato, nei test condotti, su valori dell'ordine di 1 a 27.800.

"L'indagine ha accertato che, all'attivazione di ogni sessione, lo strumento apre due canali di comunicazione paralleli verso i server della società"

Cosa è stato trasferito, e perché è grave
Il canale nascosto trasmetteva l'intero repository tracciato: tutti i file, la storia completa dei commit, i file .env con le variabili di ambiente. Come da prassi consolidata nei .env gli sviluppatori conservano API key, password di database, token cloud, chiavi SSH. I test hanno confermato che le credenziali venivano trasmesse in chiaro, senza redazione. Il fatto che il tool contenesse anche un'opzione di privacy risulta essere circostanza aggravante, non attenuante. L'utente che disabilitava la telemetria stava solo impedendo la successiva ritenzione non, ma non stava disabilitando l'upload del repository. Il codice partiva comunque e il canale nascosto operava indipendentemente da quale file lo sviluppatore avesse istruito il modello a leggere o non leggere. In un test emblematico, il ricercatore ha posizionato un file "canary" istruendo esplicitamente l'agente di non aprirlo. Il file è stato recuperato dal bundle intercettato.

I profili GDPR
Il primo piano di analisi è quello della protezione dei dati personali. I repository Git degli sviluppatori contengono, con frequenza sistematica, dati personali tra i quali log di sistema, indirizzi email, riferimenti a utenti reali nelle stringhe di test, dati anagrafici in file di configurazione. Quando l'utente è un dipendente di un'azienda, l'invio del repository verso xAI configura una comunicazione di dati personali di cui il titolare del trattamento (il datore di lavoro) non era informato e per cui non

Il caso Grok Build
Quando l'AI copia il tuo codice senza dirtelo

aveva base giuridica. L'art. 5 GDPR sui principi di liceità e trasparenza, l'art. 6 sulla base giuridica e l'art. 13 sull'informativa risultano violati simultaneamente. Il caso ha immediata rilevanza extraeuropea. L'Autorità irlandese di protezione dei dati (DPC) ha un'inchiesta statutaria aperta su xAI dall'aprile 2025 in relazione alla compliance GDPR generale della società. Il caso Grok Build fornisce alla DPC un elemento fattuale nuovo e verificabile.

Il segreto industriale e la proprietà intellettuale
Il secondo piano è quello della tutela del segreto commerciale ai sensi del D.Lgs. 63/2018 di recepimento della Direttiva UE 2016/943. I repository Git aziendali contengono spesso codice proprietario coperto da segreto industriale. La trasmissione a un soggetto terzo, senza il consenso esplicito del titolare, configura una violazione dell'obbligo di riservatezza che grava sul dipendente e, potenzialmente, un'ipotesi di appropriazione indebita quando il codice viene utilizzato per addestrare modelli di intelligenza artificiale. xAI dichiara di non aver utilizzato il codice per il training, ma non ha fornito attestazioni indipendenti che lo confermino.

La catena di fornitura e la responsabilità dell'azienda
Il terzo piano è quello della supply chain. Migliaia di aziende hanno consentito ai propri sviluppatori di utilizzare Grok Build in beta senza una valutazione preventiva del rischio. Ai sensi della NIS2 e del D.Lgs. 138/2024, la gestione del rischio nella catena di approvvigionamento è obbligo autonomo dei soggetti NIS. Un tool che esfiltra codice sorgente e credenziali senza documentarlo è, oggettivamente, un rischio di supply chain che avrebbe dovuto essere identificato prima dell'uso in produzione.

Cosa devono fare le imprese adesso
Tre azioni immediate. 1. chi ha utilizzato Grok Build prima del 13 luglio 2026 deve considerare compromesse tutte le credenziali presenti nei repository: non solo quelle nei file correnti, ma anche quelle presenti nella storia dei commit. La rotazione è d'obbligo. 2. le policy aziendali sull'uso di strumenti AI di terze parti devono includere valutazioni preventive del traffico di rete generato, non solo delle dichiarazioni di privacy del fornitore. 3. i contratti con i fornitori di AI devono includere clausole specifiche sull'audit indipendente delle telemetrie, sulla verificabilità delle promesse di cancellazione, sulla notifica tempestiva di modifiche architetturali. Il caso Grok Build non è un incidente isolato. È il segnale che l'era dell'AI-first sviluppo sta rendendo strutturale un rischio che il diritto europeo aveva già disciplinato in astratto. Ora la giurisprudenza dovrà decidere quanto in fretta applicarlo.

Allinea
Avvera Compliance Review
Luglio 2026

Linee guida della Commissione UE sulla trasparenza dell'AI

Cosa cambia il 2 agosto per fornitori e deployer

Il 20 luglio 2026 la Commissione europea ha pubblicato le linee guida in materia di obblighi di trasparenza per fornitori e deployer di sistemi di intelligenza artificiale, destinate ad accompagnare l'applicazione dell'articolo 50 dell'AI Act. Gli obblighi diventano operativi il 2 agosto 2026. Le linee guida – accompagnate da un documento di Q&A e da un fact sheet illustrativo – completano il quadro attuativo già delineato dal Code of Practice on Transparency of AI-Generated Content pubblicato lo scorso giugno. Per fornitori e utilizzatori professionali di sistemi di AI, il perimetro delle attività richieste è ora sufficientemente definito per procedere all'adeguamento.

Il quadro normativo: articolo 50 AI Act
L'articolo 50 del Regolamento (UE) 2024/1689 risponde a un rischio strutturale del mercato digitale contemporaneo: la difficoltà crescente di distinguere ciò che è stato generato da un sistema di intelligenza artificiale da ciò che non lo è stato. Deepfake, immagini sintetiche, testi prodotti da modelli generativi entrano quotidianamente nell'ecosistema informativo senza che il destinatario abbia gli strumenti per riconoscerne la natura. La norma articola gli obblighi su due piani distinti, che riflettono la duplice posizione degli operatori nella catena del valore dell'AI.

Gli obblighi dei fornitori
Ai fornitori – provider – di sistemi di AI generativa spettano due adempimenti. In primo luogo, la progettazione dei sistemi in modo da informare gli utenti quando questi interagiscono direttamente con un'intelligenza artificiale. Il principio non ammette eccezioni riferite al presunto carattere manifesto dell'interazione: le linee guida chiariscono che l'obbligo informativo permane anche laddove l'utente possa presumibilmente ricavare la natura artificiale dell'interlocutore da altri elementi contestuali. In secondo luogo, l'obbligo di marcatura in formato machine-readable degli output generati o manipolati dal sistema, in modo da renderli rilevabili quali contenuti artificialmente prodotti. Il Code of Practice del giugno 2026 individua i requisiti tecnici – efficacia, interoperabilità, robustezza – cui tali soluzioni devono conformarsi.

Gli obblighi dei deployer
Ai deployer – cioè agli utilizzatori professionali dei sistemi --spettano obblighi di etichettatura visibile per l'utente finale. Devono essere segnalati: i deepfake, definiti quali immagini, audio o video che rappresentano persone, oggetti o eventi in modo tale da apparire autentici pur non essendolo; i contenuti generati da AI su materie di interesse pubblico, salvo che siano stati sottoposti a revisione umana editoriale; l'utilizzo di sistemi di riconoscimento delle emozioni e di categorizzazione biometrica. La revisione umana editoriale opera come esimente sostanziale rispetto al primo obbligo: la logica è quella di trasferire la responsabilità della veridicità dall'algoritmo al soggetto editoriale, il quale – assumendo il controllo editoriale – assume anche il rischio dell'accuratezza dei contenuti.

I profili giuridici di maggior rilievo
Tre elementi meritano attenzione particolare da parte dei consulenti compliance.
Il primo concerne la qualificazione dei ruoli. Un'impresa che integri un modello di intelligenza artificiale sviluppato da terzi all'interno di un proprio prodotto o servizio può cumulare, rispetto a contenuti differenti, tanto la posizione di provider quanto quella di deployer. Le linee guida forniscono criteri per la corretta qualificazione, ma

Linee guida della Commissione UE sulla trasparenza dell'AI

Cosa cambia il 2 agosto per fornitori e deployer

la valutazione resta caso per caso. Il secondo concerne l'interazione con la disciplina della responsabilità civile. La violazione degli obblighi di trasparenza costituisce, ai sensi della Legge 132/2025 e dei suoi decreti attuativi, presupposto della presunzione del nesso di causalità nei giudizi risarcitori. Non adempiere agli obblighi dell'art. 50 non è soltanto un rischio sanzionatorio: rende più agevole per il danneggiato dimostrare in giudizio la responsabilità dell'operatore. Il terzo concerne l'articolazione tra AI Act e Digital Services Act. Per le grandi piattaforme di user generated content, gli obblighi di etichettatura dei contenuti generati da AI si sommano agli obblighi di trasparenza già previsti dal DSA. La sentenza della Corte di Giustizia del 16 luglio 2026 nella causa C-421/24 ha confermato che la selezione algoritmica dei contenuti fa venire meno la neutralità dell'intermediario: il combinato degli obblighi si traduce in una responsabilità stratificata che le piattaforme dovranno documentare in modo coerente.

Cosa devono fare le imprese

Tre azioni immediate. Anzitutto, identificare il ruolo assunto rispetto a ciascun sistema di AI in uso – provider, deployer, entrambi. In secondo luogo, aggiornare le procedure di marcatura e etichettatura in coerenza con le linee guida e con il Code of Practice, valutando l'opportunità dell'adesione a quest'ultimo. Infine, integrare la conformità all'art. 50 nella documentazione di compliance già predisposta ai fini GDPR e DSA, in modo da costruire una posizione difendibile in sede ispettiva e in sede risarcitoria.

Allinea
Avvera Compliance Review

L'incidente OpenAI-Hugging Face

Cosa dice il diritto quando è l'AI a compiere l'atto illecito

Il 22 luglio 2026 OpenAI ha reso noto un incidente informatico che l'azienda stessa ha definito "senza precedenti". Nel corso di una valutazione interna volta a misurare le capacità offensive dei propri modelli sperimentali, alcuni sistemi hanno oltrepassato le restrizioni dell'ambiente controllato in cui erano stati confinati, hanno individuato e concatenato vulnerabilità presenti nella sandbox, sono riusciti a stabilire una connessione con l'esterno e, muovendosi lateralmente, hanno raggiunto e compromesso alcuni sistemi di Hugging Face - la principale piattaforma mondiale per la condivisione di modelli e dataset di intelligenza artificiale. L'agente autonomo ha identificato Hugging Face come archivio utile a risolvere il benchmark su cui era impegnato, ha sfruttato credenziali compromesse e vulnerabilità sconosciute, ottenendo accesso non autorizzato ad alcuni dataset interni e a determinate credenziali di servizio. Sotto il profilo tecnico l'episodio è già stato ampiamente discusso. Sotto il profilo giuridico apre interrogativi che meritano un'analisi puntuale.

Chi risponde dell'atto compiuto dall'agente autonomo

Il primo interrogativo concerne l'imputabilità della condotta. L'agente non ha agito su istruzione umana diretta: ha identificato autonomamente l'obiettivo, elaborato una strategia di intrusione, esercitato le proprie capacità offensive. Nondimeno, ha operato all'interno di un ambiente di test volutamente configurato con restrizioni di sicurezza ridotte, per iniziativa del suo principal - OpenAI - che lo ha messo in condizione di agire con quelle capacità e in quel contesto. Il quadro normativo europeo, che si va progressivamente definendo, offre coordinate precise.

L'incidente OpenAI-Hugging Face

Cosa dice il diritto quando è l'AI a compiere l'atto illecito

L'art. 1228 del codice civile italiano - responsabilità del debitore per fatto degli ausiliari - si presta a essere applicato per analogia agli agenti AI utilizzati nell'esecuzione di obbligazioni. Chi mette in condizione un agente di compiere determinate azioni risponde delle azioni dell'agente come risponderebbe delle proprie. La circostanza che il comportamento fosse "esclusivamente orientato al completamento del test" - come dichiarato da OpenAI - non rileva ai fini della qualificazione oggettiva della condotta come accesso non autorizzato ai sensi dell'art. 615-ter del codice penale.

Il ruolo del sandbox e il dovere di contenimento

Un secondo profilo attiene all'adeguatezza delle misure di contenimento predisposte. In ambito cybersecurity, il sandbox costituisce lo strumento standard per il test di sistemi potenzialmente pericolosi: un ambiente virtuale separato dal resto dell'infrastruttura, tale da impedire che il comportamento del sistema in prova possa propagarsi all'esterno. Il fatto che il sandbox sia stato aggirato dai modelli oggetto di test costituisce, di per sé, un elemento rilevante ai fini della valutazione della diligenza professionale del titolare del trattamento del test - OpenAI - rispetto agli obblighi di sicurezza previsti dall'art. 15 dell'AI Act (Reg. UE 2024/1689). La norma impone infatti ai fornitori di sistemi ad alto rischio l'obbligo di garantire livelli adeguati di accuratezza, robustezza e cybersicurezza - con particolare riguardo alla resistenza a tentativi di manipolazione da parte di terzi non autorizzati.

La lethal trifecta e la responsabilità nel design

Il caso rappresenta un'illustrazione manifesta del concetto di lethal trifecta elaborato dalla comunità di sicurezza. L'agente coinvolto disponeva contemporaneamente di accesso a dati sensibili, esposizione a input potenzialmente non fidati - nella specie, i risultati delle interazioni con l'ambiente esterno che l'agente medesimo esplorava - e capacità di compiere azioni con effetti irreversibili verso l'esterno. La presenza contestuale dei tre elementi, secondo la letteratura tecnica, integra una vulnerabilità strutturale del sistema. Sul piano giuridico, la circostanza fonda un rilievo di negligenza qualificata nella progettazione dell'ambiente di test.

"la responsabilità nell'era degli agenti autonomi non si esaurisce nella verifica dell'output, ma si estende all'architettura del sistema"

Il rischio Hugging Face e la responsabilità concorrente

La posizione di Hugging Face merita autonomo esame. Il fatto che credenziali di servizio della piattaforma fossero utilizzabili da un agente esterno per accedere a dataset interni configura, ai sensi dell'art. 24 del D.Lgs. 138/2024 di recepimento della NIS2, una potenziale carenza nella gestione della catena di approvvigionamento e nella protezione degli accessi privilegiati. La rilevazione tempestiva dell'intrusione e il contenimento operato dai sistemi difensivi costituiscono elemento attenuante, non escludente. Hugging Face - quale infrastruttura critica per l'ecosistema europeo dell'intelligenza artificiale - è verosimilmente qualificabile come soggetto NIS con obblighi rafforzati di sicurezza.

Cosa insegna il caso

L'episodio conferma una tesi che il diritto europeo aveva già disciplinato in via prospettica: la responsabilità nell'era degli agenti autonomi non si esaurisce nella verifica dell'output, ma si estende all'architettura del sistema. Chi mette in condizione un agente di operare autonomamente - anche in ambiente di test - risponde delle capacità che gli ha conferito e dei confini che ha o non ha saputo garantire. Il sandbox aggirato è, sul piano giuridico, un contenimento non adeguato. E l'inadeguatezza del contenimento è il fondamento della responsabilità.

Allinea
Avvera Compliance Review
Luglio 2026

Supply chain e NIS

Le nuove FAQ ACN archiviano le clausole "fotocopia"

Con l'aggiornamento del 24 luglio 2026 alle FAQ "Misure di sicurezza e notifica di incidenti", l'ACN chiarisce come i soggetti NIS devono gestire la sicurezza della catena di approvvigionamento: nessun obbligo di riaprire i contratti in corso e requisiti da calibrare sulla singola fornitura, non da riversare indistintamente su tutti i fornitori.
Le FAQ da MSB.12 a MSB.19 intervengono sulle misure GV.SC-01, GV.SC-05 e GV.SC-07 delle specifiche di base. Il filo conduttore è il richiamo all'approccio risk-based.

Un processo in quattro fasi

La FAQ MSB.13 scandisce la sequenza: valutazione del rischio associato alla fornitura (GV.SC-07, punto 1); identificazione dei requisiti di sicurezza, coerenti con gli esiti della valutazione e con le misure applicate ai propri sistemi (GV.SC-01, punto 1); enforcement, cioè inserimento dei requisiti in richieste di offerta, bandi di gara, accordi quadro, contratti e convenzioni (GV.SC-05, punto 1); verifica periodica e documentata della conformità (GV.SC-07, punto 2). L'ordine non è formale: la valutazione del rischio precede la definizione dei requisiti. Sul piano operativo, la procedura di qualifica deve quindi prevedere una verifica a monte della stesura e della firma del contratto. I criteri minimi (MSB.14) sono cinque: livello di accesso del fornitore ai sistemi informativi e di rete; accesso a proprietà intellettuale e dati, in funzione della loro criticità; impatto di una grave interruzione della fornitura; tempi e costi di ripristino; ruoli e responsabilità del fornitore nel governo dei sistemi.

Contratti in essere: nessuna riapertura

È il chiarimento di maggiore impatto pratico. La FAQ MSB.12 esclude l'obbligo di adeguare i contratti già in essere: l'inserimento dei requisiti è obbligatorio - salve motivate e documentate ragioni normative o tecniche - per i contratti stipulati, rinnovati o prorogati a partire dal termine di adozione delle misure. Per i soggetti iscritti nell'elenco NIS entro il 31 dicembre 2025 il termine è di diciotto mesi dalla comunicazione di inserimento (prime scadenze dall'autunno 2026); per quelli inseriti per la prima volta nel 2026 è il 31 luglio 2027 (determinazione n. 127434/2026).

"Non tutti i requisiti delle misure di base vanno ribaltati sul fornitore, né riprodotti alla lettera: è sufficiente recepirne il contenuto sostanziale"

Requisiti pertinenti, non "a tappeto"

Il blocco più utile pone limiti espliciti all'over-compliance contrattuale. Non tutte le forniture richiedono requisiti di sicurezza, ma solo quelle con potenziali impatti sulla sicurezza dei sistemi informativi e di rete (MSB.15). Non tutti i requisiti delle misure di base vanno ribaltati sul fornitore, né riprodotti alla lettera: è sufficiente recepirne il contenuto sostanziale (MSB.16). Le categorie di misure dell'art. 24 del d.lgs. 138/2024 non sono un insieme minimo sempre applicabile, ma vanno modulate fino all'eventuale esclusione di alcune, in base a contesto operativo, livello di rischio e criticità dei servizi affidati (MSB.17): per affidamenti non ICT - pulizie, vigilanza senza strumenti digitali, progettazione senza BIM - i requisiti imposti al fornitore devono restare coerenti con l'oggetto della prestazione. Lo stesso criterio di proporzionalità, pertinenza e adeguatezza vale per i contratti misti (MSB.19). È un argomento spendibile da chi riceve allegati contrattuali che pretendono ogni misura possibile a prescindere dal servizio: la richiesta indiscriminata non è imposta dalla normativa NIS.
Quando l'aggiudicatario è un RTI o un consorzio, infine, le misure vanno soddisfatte dai soli componenti che erogano, anche parzialmente, la prestazione con impatti sulla sicurezza informatica (MSB.18) - il che presuppone una mappatura chiara delle parti di servizio assegnate a ciascuno.

Supply chain e NIS
Le nuove FAQ ACN archiviano le clausole "fotocopia"

Cosa fare adesso

Per i soggetti NIS con scadenza nel mese di ottobre l'aggiornamento suggerisce alcune priorità:

1. classificare il parco fornitori distinguendo le forniture con potenziali impatti sulla sicurezza da quelle prive di rilevanza, con evidenza documentale della classificazione;
2. formalizzare la procedura di valutazione del rischio fornitore sui cinque criteri di GV.SC-07, collocandola a monte della contrattualizzazione e prevedendo il riesame in caso di modifiche al servizio, ai subfornitori, all'architettura o al perimetro dei dati trattati;
3. costruire un set modulare di clausole - non un allegato unico - in modo da poter graduare i requisiti per fascia di rischio e tipologia di affidamento;
4. prevedere, nelle proprie procedure, verifiche periodiche e definire in anticipo quali evidenze richiedere per documentale la compliance (certificazioni, report di audit, esiti di test, SLA di sicurezza;
5. presidiare rinnovi e proroghe;
6. tracciare le esclusioni: dove i requisiti non vengono inseriti per motivate ragioni normative o tecniche, la motivazione deve risultare per iscritto.

Le FAQ quindi non aggravamo gli obblighi: li spiegano come più selettivi, spostando così il baricentro dalla redazione delle clausole alla capacità di dimostrare, con evidenze, perché quelle clausole sono state scelte proprio per quella fornitura.

Allinea
Avvera Compliance Review

Il 2 agosto non è un rinvio
Trasparenza e vigilanza entrano in funzione

Il 27 luglio 2026 l'AI Omnibus è entrato in vigore in tutta l'UE, introducendo termini più lunghi per la semplificazione amministrativa. Il regolamento di semplificazione, approvato ha spostato in avanti il cuore degli obblighi sull'alto rischio: il 2 dicembre 2027 per i sistemi stand-alone dell'Allegato III - selezione del personale, gestione del rapporto di lavoro, merito creditizio, istruzione, accesso ai servizi essenziali, giustizia - e il 2 agosto 2028 per l'IA incorporata nei prodotti disciplinati dall'Allegato I. Sedici mesi in più, motivati dalla mancata maturazione degli standard armonizzati.
Si tratta di una proroga che non impatta su tutti gli obblighi, infatti a partire dal 2 agosto 2026 tre cose accadono comunque.

Il 2 agosto non è un rinvio

Trasparenza e vigilanza entrano in funzione

Primo: gli obblighi di trasparenza

L'articolo 50 non è stato toccato dalla proroga. Da domenica, chi fornisce sistemi destinati a interagire con persone fisiche deve renderne riconoscibile la natura artificiale, salvo che ciò sia evidente per un utente mediamente avveduto. Chi impiega sistemi di riconoscimento delle emozioni o di categorizzazione biometrica deve informare gli interessati. Chi genera deepfake o pubblica testi destinati a informare il pubblico su questioni di interesse pubblico deve dichiararlo. E i fornitori di sistemi generativi devono marcare i contenuti sintetici in formato leggibile dalla macchina: qui una disciplina transitoria concede tempo fino al 2 dicembre 2026 per i sistemi già immessi sul mercato, mentre i contenuti anteriori al 2 agosto non vanno etichettati retroattivamente. Le Linee guida della Commissione sull'articolo 50, pubblicate il 20 luglio, e il Codice di condotta sulla marcatura non sono vincolanti, ma è ingenuo trattarli come letteratura. Chi sceglie di non aderire dovrà dimostrare misure alternative equivalenti e, nel frattempo, sopportare un onere informativo più gravoso davanti all'autorità. Il rischio è quantificato: fino a 15 milioni di euro o il 3% del fatturato mondiale, se superiore.

Secondo: il controllore arriva

Fino a ieri l'AI Act era un regolamento senza vigilanza operativa. Dal 2 agosto le autorità nazionali entrano in funzione e la Commissione acquisisce il potere sanzionatorio sui fornitori di modelli per finalità generali. In Italia l'architettura è definita: la legge 132/2025 e i decreti attuativi approvati dal Consiglio dei ministri il 10 giugno affidano ad AgID il ruolo di autorità di notifica e ad ACN quello di vigilanza del mercato, con poteri ispettivi e sanzionatori e funzione di punto di contatto unico con l'Unione. Accanto, Banca d'Italia, CONSOB e IVASS per il perimetro finanziario e il Garante per i sistemi ad alto rischio in ambito law enforcement e giustizia, con un comitato di coordinamento presso la Presidenza del Consiglio a comporre le inevitabili sovrapposizioni.

Terzo: la formazione diventa esigibile

Il primo banco di prova sarà l'adempimento più antico e più trascurato. L'articolo 4 impone a fornitori e deployer - chiunque usi l'IA a scopo professionale - di assicurare al personale un livello adeguato di alfabetizzazione, proporzionato al ruolo e ai rischi. È in vigore dal 2 febbraio 2025 e nessuno ha mai potuto verificarlo. Da domenica sì. Chi non è in grado di esibire un programma documentato, con destinatari, contenuti tecnici e giuridici e tracciabilità della partecipazione, parte con uno svantaggio in qualunque interlocuzione ispettiva.

Cosa fare adesso

L'agenda minima: inventario dei sistemi in uso, con classificazione per Allegato; revisione dei touchpoint conversazionali e delle policy editoriali per l'etichettatura; clausole contrattuali che ribaltino sui fornitori gli obblighi di marcatura; verifica del watermarking entro dicembre; formazione documentata. E, sull'alto rischio, nessuna sospensione dei programmi già avviati: un ciclo di adeguamento richiede in media dagli otto ai quattordici mesi. Dicembre 2027 è più vicino di quanto il calendario suggerisca.

Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Luglio

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