Agenti AI e harness: chi risponde quando la macchina decide?

Allinea

Avvera Compliance Review

Maggio 2026

Poste Italiane e Postepay sanzionate dal Garante

AI ACT Omnibus

Accessi abusivi alle banche dati dello Stato

Linee guida sulla classificazione dei sistemi AI ad alto rischio

Tracking Pixel nelle e-mail

Licenziare per l'AI: cosa è già lecito, cosa è ancora controverso e cosa manca

L'AI accelera il crimine informatico

Allinea
Avvera Compliance Review
Maggio 2026

Poste Italiane e Postepay sanzionate dal Garante: quando l'antifrode diventa sorveglianza

Con il provvedimento n. 237 del 17 aprile 2026, il Garante per la protezione dei dati personali ha sanzionato Poste Italiane S.p.a. e PostePay S.p.a. per i trattamenti di dati personali effettuati tramite le app Bancoposta e PostePay su sistema operativo Android. Al centro della vicenda c'è una libreria software antifrode che, nella configurazione adottata dalle due società, accedeva all'elenco delle applicazioni installate e in esecuzione sui dispositivi degli utenti. L'obiettivo dichiarato era rilevare malware. Il risultato, per il Garante, era una sorveglianza sproporzionata e priva di adeguata base giuridica.

I fatti

Nell'aprile 2024 pervennero all'Autorità 140 segnalazioni e 12 reclami. Gli utenti delle due app avevano ricevuto un messaggio che li invitava ad autorizzare l'accesso ai propri "dati di utilizzo", qualificandolo come obbligatorio e avvertendo che, in caso di mancata attivazione, l'operatività dell'app sarebbe stata inibita dopo tre accessi. L'autorizzazione consentiva alle app di monitorare le applicazioni in uso sul dispositivo, la loro frequenza d'uso, il gestore telefonico e altre informazioni di utilizzo tramite la libreria in questione, che raccoglieva i codici hash MD5 delle app in esecuzione e li trasmetteva ai sistemi cloud del responsabile del trattamento.

Il nodo giuridico: base giuridica errata e consenso non valido

Le società sostenevano che il trattamento fosse esentato dal consenso in quanto strettamente necessario all'erogazione del servizio, ai sensi dell'art. 122 del Codice Privacy, e che trovasse fondamento nell'obbligo legale derivante dalla normativa PSD2 e dai relativi standard tecnici EBA. Il Garante ha respinto entrambe le argomentazioni. Sul primo punto, l'Autorità ha chiarito che l'esonero dal consenso previsto dall'art. 122 è di stretta interpretazione e si applica solo alle operazioni tecnicamente indispensabili all'erogazione del servizio richiesto. L'accesso all'elenco delle app installate, che può rivelare condizioni di salute, orientamenti religiosi o politici, abitudini finanziarie e aspetti della vita privata, non è strettamente necessario al funzionamento di un'app bancaria. Lo conferma un dato emerso dall'istruttoria dell'AGCM: nei primi sette mesi di utilizzo del sistema, le società stesse avevano dichiarato che la nuova funzionalità non aveva prodotto una rilevazione maggiore o più efficiente di fenomeni fraudolenti. E, soprattutto, le società avevano successivamente disabilitato la funzionalità senza particolari disfunzioni operative. Sul secondo punto, il Garante ha precisato che la normativa PSD2 non impone la specifica configurazione adottata dalle società. Impone misure antifrode, non quella misura. Meccanismi alternativi (es. autenticazione multi-fattore rafforzata, algoritmi di scoring anonimi, controlli runtime, monitoraggi di rete) avrebbero potuto garantire un livello di sicurezza equivalente con un impatto molto inferiore sulla sfera personale degli utenti.

" L'accesso all'elenco delle app installate non è strettamente necessario al funzionamento di un'app bancaria"

Privacy by design violata e DPIA assente

Le violazioni accertate vanno oltre la questione della base giuridica. Il Garante ha contestato l'assenza di una valutazione d'impatto preventiva adeguata rispetto alla specifica configurazione adottata, la non conformità dell'informativa resa agli utenti, che non descriveva con sufficiente precisione le modalità e le finalità del trattamento, il mancato rispetto del principio di limitazione della conservazione, con dati conservati per periodi superiori a quanto inizialmente dichiarato, e profili di inadeguatezza nella designazione del responsabile del trattamento e nella catena dei sub-responsabili.

Poste Italiane e Postepay sanzionate dal Garante: quando l'antifrode diventa sorveglianza

La violazione del principio di privacy by design è quella che il Garante sottolinea con maggiore energia: una soluzione modulare e configurabile avrebbe potuto essere adottata in una configurazione meno invasiva. La scelta della configurazione più ampia non rispondeva a un requisito normativo, ma a una decisione organizzativa.

Le implicazioni per le imprese

Il provvedimento ha una portata che va oltre Poste Italiane. Chiunque integri librerie di terze parti nei propri sistemi per finalità di sicurezza o antifrode deve verificare che la configurazione specifica adottata sia proporzionata alle finalità dichiarate, che la base giuridica sia correttamente identificata, distinguendo tra accesso al dispositivo e trattamenti successivi, e che la DPIA sia stata effettuata rispetto al trattamento concreto, non a quello astratto. La sicurezza informatica è un obbligo. Non è una giustificazione per raccogliere più dati di quanti ne servano.

Allinea
Avvera Compliance Review
Maggio 2026

AI Act Omnibus: l'accordo del 7 maggio 2026 tra Parlamento e Consiglio. Cosa cambia davvero per le imprese?

Nella notte tra il 6 e il 7 maggio 2026, Parlamento europeo e Consiglio dell'Unione europea hanno raggiunto un accordo provvisorio sulla proposta di modifica dell'AI Act, nell'ambito del pacchetto legislativo Digital Omnibus proposto dalla Commissione nel novembre 2025. L'accordo, che dovrà essere formalmente adottato entro il 2 agosto 2026, non riscrive l'impianto del Regolamento, ma lo calibra spostando scadenze, riducendo sovrapposizioni normative, aggiungendo un divieto nuovo e rafforzando la governance centralizzata.

Le nuove scadenze per i sistemi ad alto rischio

Il punto più atteso riguarda il calendario. Le nuove date di applicazione degli obblighi per i sistemi ad alto rischio sono il 2 dicembre 2027 per i sistemi autonomi (inclusi biometria, infrastrutture critiche, istruzione, occupazione e forze dell'ordine) e il 2 agosto 2028 per i sistemi integrati come componenti di sicurezza in prodotti soggetti a normativa settoriale. Un rinvio di circa un anno, motivato dalla necessità di attendere standard tecnici e linee guida prima che gli obblighi più complessi entrino in vigore. Gli obblighi di AI literacy (in vigore dal febbraio 2025) e quelli sui modelli GPAI restano invariati.

Il watermarking e il divieto dei sistemi nudifier

L'accordo riduce da sei a tre mesi il periodo per implementare soluzioni di trasparenza sui contenuti generati artificialmente, con scadenza al 2 dicembre 2026. Non è una proroga: è un riallineamento del calendario agli strumenti effettivamente disponibili, per evitare un vuoto applicativo in attesa degli standard europei. Sul fronte dei nuovi divieti, l'accordo introduce il bando esplicito dei sistemi di AI progettati per generare contenuti sessuali e intimi non consensuali o materiale pedopornografico (immagini, video e audio sintetici). Il divieto si applica sia a chi sviluppa sia a chi distribuisce questi sistemi nel mercato europeo. Scadenza di adeguamento: 2 dicembre 2026.

AI Act Omnibus: l'accordo del 7 maggio 2026 tra Parlamento e Consiglio. Cosa cambia davvero per le imprese?

Le semplificazioni per le imprese
L'accordo chiarisce l'interazione tra l'AI Act e le normative settoriali. Regolamento Macchine, dispositivi medici, giocattoli eliminando la doppia conformità che aveva generato le maggiori preoccupazioni dell'industria. Viene ristretta la definizione di "componente di sicurezza": i sistemi puramente assistivi non ricadono automaticamente nel regime ad alto rischio. Le esenzioni per le PMI vengono estese alle small mid-cap. Viene introdotta la possibilità di trattare dati personali per correggere bias, purché strettamente necessario e con garanzie adeguate.

Cosa devono fare adesso le imprese
Il primo passo è aggiornare la mappatura dei propri sistemi alla luce delle nuove scadenze. Chi aveva pianificato la conformità entro il 2 agosto 2026 per i sistemi ad alto rischio deve ricalcolare: la data è ora il 2 dicembre 2027 per i sistemi autonomi e il 2 agosto 2028 per quelli integrati in prodotti soggetti a normativa settoriale. Non è un'autorizzazione a rallentare, ma è un'indicazione su dove concentrare le risorse nell'immediato. Il secondo passo riguarda chi opera in settori già coperti da normativa settoriale specifica. L'accordo chiarisce che non si applica la doppia conformità: è sufficiente rispettare le regole settoriali esistenti. Va verificato caso per caso se il proprio sistema rientra in questo perimetro, perché la valutazione non è automatica. Il terzo passo è obbligatorio per chi sviluppa o distribuisce sistemi generativi. Il divieto sui sistemi nudifier è immediato nella sua portata normativa: riguarda chiunque offra un sistema generativo utilizzabile per produrre quel tipo di contenuti senza adeguate misure di sicurezza. La responsabilità è del fornitore, non dell'utente finale. Il quarto passo riguarda il watermarking: il 2 dicembre 2026 è la scadenza per implementare strumenti di rilevazione e tracciamento dei contenuti generati artificialmente. Chi non ha ancora avviato la valutazione tecnica deve farlo adesso: tre mesi sono un margine operativo stretto per chi parte da zero. Il Digital Omnibus non ha reso l'AI Act meno esigente. Ha reso le scadenze più realistiche e le regole più leggibili. La conformità resta un obbligo con date precise e conseguenze definite.

"Il Digital Omnibus non ha reso l'AI Act meno esigente. Ha reso le scadenze più realistiche e le regole più leggibili"

Allinea
Avvera Compliance Review
Maggio 2026

Accessi abusivi alle banche dati dello Stato: il mercato nero delle informazioni riservate

Nella mattina del 13 maggio 2026, la Procura di Napoli diretta da Nicola Gratteri ha sgominato un'organizzazione criminale dedita all'accesso abusivo a sistemi informatici istituzionali, alla corruzione e alla rivelazione di segreto d'ufficio. L'operazione ha interessato le province di Napoli, Roma, Ferrara, Belluno e Bolzano, con dieci arresti, di cui quattro in carcere e sei ai domiciliari, e altri diciannove destinatari di misure cautelari. Sono stati eseguiti sequestri per circa 1,3 milioni di euro.

Il meccanismo: credenziali di servizio come strumento di commercio illecito
Il punto di partenza dell'indagine è stato il rilevamento di un volume di accessi anomalo: due agenti di polizia avevano effettuato rispettivamente 600.000 e 130.000 accessi alle banche dati riservate nell'arco di due anni, nessuno dei quali giustificato da esigenze di servizio. Non si trattava di un attacco informatico nel senso tecnico del termine (nessuna vulnerabilità sfruttata, nessun sistema violato dall'esterno). Gli agenti utilizzavano le proprie credenziali istituzionali per accedere a banche dati cui erano autorizzati per ragioni di servizio, estraendo informazioni che non avevano alcun titolo a consultare per finalità personali o commerciali.

Accessi abusivi alle banche dati dello Stato: il mercato nero delle informazioni riservate

Il sistema è strutturato e prevede tariffe. Per una verifica nella banca dati SDI (il sistema di indagine del Ministero dell'Interno) il compenso era di 25 euro. Gli accessi ai dati INPS costavano tra i 6 e gli 11 euro, a seconda del documento richiesto. Le informazioni così ottenute venivano cedute a una decina di società, alcune dislocate al Nord, che le richiedevano con cadenza quasi quotidiana. Sul server sequestrato nella notte tra il 12 e il 13 maggio sono stati trovati oltre un milione di dati conservati.

I soggetti coinvolti e le banche dati violate

Oltre agli agenti della Polizia di Stato, risultano coinvolti dipendenti dell'INPS, dell'Agenzia delle Entrate e due direttori di filiali di Poste Italiane. Le banche dati interessate includono il Sistema di indagine del Ministero dell'Interno, i database previdenziali dell'INPS e quelli dell'Agenzia delle Entrate. Si tratta di archivi che contengono dati personali di elevata sensibilità: situazioni patrimoniali, pendenze fiscali, precedenti penali, informazioni anagrafiche dettagliate. Tra gli indagati figura anche una persona riconducibile all'agenzia Equalize di Milano, già coinvolta in altre inchieste analoghe.

I profili giuridici rilevanti

Il caso solleva almeno tre questioni che vanno ben oltre la cronaca giudiziaria. La prima riguarda il controllo degli accessi privilegiati nelle pubbliche amministrazioni. Il volume di 730.000 accessi in due anni (una media di quasi mille al giorno) avrebbe dovuto attivare meccanismi automatici di anomaly detection molto prima che l'indagine li intercettasse. La presenza di sistemi di monitoraggio dei log di accesso è un requisito minimo di sicurezza informatica: che nessun alert abbia segnalato in tempo reale un'attività di questa portata è di per sé una vulnerabilità sistemica. La seconda questione riguarda il GDPR e la responsabilità delle amministrazioni titolari del trattamento. Le banche dati violate conservano dati personali per i quali le rispettive amministrazioni sono titolari del trattamento. L'accesso abusivo da parte di soggetti interni – anche se formalmente autorizzati all'accesso per ragioni di servizio – configura una violazione dei dati personali ai sensi dell'art. 33 del GDPR, con obbligo di notifica al Garante entro 72 ore dalla conoscenza dell'evento e, nei casi più gravi, obbligo di comunicazione agli interessati. La terza questione riguarda il mercato finale delle informazioni. Come ha sottolineato il procuratore Gratteri, il mercato delle informazioni riservate è ancora vivissimo: le agenzie che raccogliendo informazioni riservate per cederle a terzi non sono un fenomeno marginale. Chi commissiona questi accessi, anche senza sapere che avvengono in modo illecito, si espone a responsabilità penali e civili che non si esauriscono nella posizione del fornitore. Il caso di Napoli è l'ennesima dimostrazione che la minaccia più difficile da gestire non viene dall'esterno dei sistemi, ma dall'interno: da chi ha le credenziali, conosce i processi e sa esattamente dove cercare. Contro questo tipo di rischio, le misure tecniche di perimetro non bastano. Serve una governance degli accessi privilegiati che tracci, analizzi e reagisca in tempo reale.

"La presenza di sistemi di monitoraggio dei log di accesso è un requisito minimo di sicurezza informatica"

Allinea
Avvera Compliance Review
Maggio 2026

Linee guida sulla classificazione dei sistemi AI ad alto rischio: la Commissione europea chiarisce l'art. 6

Il 19 maggio 2026 la Commissione europea ha pubblicato la bozza delle linee guida sulla classificazione dei sistemi AI ad alto rischio ai sensi dell'articolo 6 dell'AI Act. Il documento era atteso entro il 2 febbraio 2026 e arriva con tre mesi di ritardo. Ma arriva in un momento cruciale: molte organizzazioni non hanno ancora una risposta certa su come classificare i propri sistemi.

Il nodo: quando un sistema nell'Allegato III non è ad alto rischio

L'art. 6 individua due categorie di sistemi ad alto rischio. La prima comprende i sistemi che costituiscono componenti di sicurezza di prodotti soggetti a legislazione UE elencata nell'Allegato I e che richiedono valutazione di conformità da parte di terzi. La seconda comprende i sistemi negli ambiti dell'Allegato III: infrastrutture critiche, istruzione, occupazione, servizi essenziali, forze dell'ordine, migrazione, giustizia. Il nodo interpretativo è nel comma 3: un sistema che ricade nell'Allegato III non è automaticamente ad alto rischio se non pone un rischio significativo per la salute, la sicurezza o i diritti fondamentali, incluso il caso in cui non influenzi materialmente l'esito di un processo decisionale. Fino ad oggi, tracciare quel confine era rimasto a carico dei provider senza indicazioni operative.

Cosa chiariscono le linee guida

Le linee guida forniscono esempi pratici di sistemi che devono e non devono essere classificati come ad alto rischio per ciascuno degli ambiti dell'Allegato III. Non è una lista tassativa – gli esempi potranno essere aggiornati – ma è il primo riferimento operativo che traduce le categorie astratte del Regolamento in casi concreti. Vengono precisati anche i quattro criteri che escludono l'alto rischio: il sistema svolge un compito procedurale strettamente delimitato; migliora il risultato di un'attività umana precedente senza sostituirla; rileva pattern decisionali senza influenzare in modo significativo la valutazione umana; svolge un compito preparatorio per una valutazione condotta da una persona. In questi casi la classificazione come alto rischio può essere esclusa. Il documento è articolato in tre sezioni scaricabili separatamente: principi generali, sistemi dell'Allegato I e sistemi dell'Allegato III. Chi opera in un settore specifico può consultare solo la sezione pertinente.

Tre azioni immediate

1. Leggere la sezione dell'Allegato III relativa al proprio settore e verificare se i sistemi in uso rientrano negli esempi ad alto rischio o in quelli esclusi. Non è una verifica solo tecnica: richiede il coinvolgimento del team legale e del DPO.
2. Documentare la valutazione. L'art. 6(4) impone ai provider che ritengono il proprio sistema non ad alto rischio di documentare questa valutazione prima di immettere il sistema sul mercato. La documentazione deve essere disponibile su richiesta delle autorità di vigilanza.
3. Monitorare la versione definitiva. Le linee guida sono in bozza: chi ha già avviato la classificazione dovrà verificare che le conclusioni reggano anche alla luce del testo finale.

Le linee guida non risolvono tutte le ambiguità, ma riducono significativamente l'area grigia in cui molte organizzazioni operavano.

Allinea
Avvera Compliance Review
Maggio 2026

Tracking pixel nelle e-mail: le nuove Linee guida del Garante Privacy

Con il Provvedimento del 17 aprile 2026, il Garante per la Protezione dei Dati Personali ha adottato le nuove "Linee guida in materia di utilizzo di tracking pixel nelle comunicazioni di posta elettronica", intervenendo su un tema di particolare rilevanza per le attività di e-mail marketing e marketing automation.
Il Provvedimento si inserisce nel più ampio quadro normativo relativo alla protezione dei dati personali e all'utilizzo degli strumenti di tracciamento nelle comunicazioni elettroniche, con l'obiettivo di rafforzare il livello di trasparenza nei confronti degli utenti e chiarire le condizioni di liceità del trattamento dei dati raccolti tramite tracking pixel. Nelle Linee guida, il Garante qualifica il tracking pixel come uno strumento di tracciamento soggetto alla disciplina prevista dall'art. 122 del Codice Privacy, analogamente ai cookie e agli altri strumenti che consentono di accedere a informazioni archiviate nel terminale dell'utente o di raccogliere dati relativi all'utilizzo dei servizi digitali.

Secondo l'Autorità, infatti, tali tecnologie consentono di monitorare il comportamento del destinatario della comunicazione e-mail attraverso la raccolta di informazioni relative, ad esempio, all'apertura del messaggio, al numero di visualizzazioni, al momento della consultazione, al dispositivo utilizzato o ad ulteriori elementi tecnici connessi alla fruizione della comunicazione.

"Il Provvedimento ha l'obiettivo di rafforzare il livello di trasparenza nei confronti degli utenti e chiarire le condizioni di liceità del trattamento dei dati raccolti tramite tracking pixel"

Particolare attenzione viene dedicata al tema della trasparenza informativa. Il Garante evidenzia, infatti, che il tracking pixel costituisce uno strumento normalmente non percepibile dall'utente e, proprio per questa caratteristica, richiede specifici presidi sotto il profilo informativo. Le organizzazioni che utilizzano tali strumenti devono, quindi, assicurare che gli interessati siano adeguatamente informati circa la presenza di meccanismi di tracciamento nelle comunicazioni e-mail, le finalità perseguite tramite il monitoraggio, le modalità di utilizzo dei dati raccolti e le opzioni disponibili per esercitare i propri diritti o revocare le scelte effettuate. Le Linee guida non introducono un divieto generalizzato di utilizzo dei tracking pixel, ma distinguono in modo netto tra utilizzi tecnici o strettamente necessari e utilizzi finalizzati ad attività di marketing o profilazione comportamentale. In particolare, il Garante ritiene generalmente compatibili con le deroghe previste dall'art. 122 del Codice Privacy gli utilizzi connessi a finalità statistiche aggregate e anonimizzate, alle esigenze di sicurezza informatica, alla prevenzione delle frodi, nonché all'invio di comunicazioni istituzionali o strettamente funzionali all'erogazione di un servizio richiesto dall'utente. Diversamente, il consenso preventivo dell'interessato è richiesto nei casi in cui il tracking venga utilizzato per monitorare le aperture individuali delle e-mail, analizzare le interazioni dei destinatari, valutare le performance delle campagne marketing, segmentare gli utenti o personalizzare contenuti, frequenza e modalità delle comunicazioni sulla base dei comportamenti osservati. Secondo il Garante, rientrano, inoltre, nell'ambito delle attività soggette a consenso i trattamenti finalizzati a ricavare interessi, preferenze o propensioni commerciali dell'utente attraverso l'analisi delle informazioni raccolte tramite i pixel di tracciamento. Di particolare interesse risulta il passaggio delle Linee guida dedicato al rapporto tra consenso marketing e consenso al tracking. Il Garante ritiene, infatti, possibile che il consenso al tracciamento sia ricompreso nell'ambito del più generale consenso alle attività di marketing, purché l'interessato sia informato in modo chiaro e specifico circa la presenza di strumenti di monitoraggio e le finalità perseguite attraverso tali tecnologie.

Tracking pixel nelle e-mail: le nuove Linee guida del Garante Privacy

Viene, altresì, ribadita la necessità che le richieste di consenso siano formulate con modalità comprensibili e non fuorvianti, evitando formulazioni generiche o eccessivamente tecniche. Un ulteriore profilo centrale del Provvedimento riguarda la revoca del consenso e la necessità di garantire agli utenti un controllo effettivo sulle attività di tracciamento. Secondo il Garante, l'interessato deve poter revocare agevolmente il consenso alle attività di marketing oppure opporsi specificamente al monitoraggio tramite tracking pixel, continuando eventualmente a ricevere le comunicazioni senza essere sottoposto a forme di profilazione o analisi comportamentale. Le Linee guida incoraggiano, pertanto, l'adozione di strumenti che consentano una gestione semplice e granulare delle preferenze privacy direttamente dalle comunicazioni e-mail o attraverso aree dedicate messe a disposizione dagli operatori. Sotto il profilo operativo, il Provvedimento richiama l'attenzione delle organizzazioni sulla necessità di verificare attentamente le configurazioni delle piattaforme di marketing automation e dei servizi utilizzati per l'invio delle comunicazioni elettroniche, al fine di assicurare che i meccanismi di tracciamento siano coerenti con le scelte di consenso espresse dagli utenti e che non vengano effettuate attività di monitoraggio in assenza di una valida base giuridica. Le nuove Linee guida confermano, nel complesso, il crescente livello di attenzione delle Autorità di controllo verso gli strumenti di tracciamento impiegati nelle comunicazioni digitali e rappresentano un ulteriore passo nel percorso di rafforzamento delle tutele in materia di protezione dei dati personali, imponendo alle organizzazioni una revisione delle proprie pratiche informative, dei meccanismi di raccolta del consenso e dei processi di gestione delle preferenze degli utenti.

Allinea
Avvera Compliance Review
Maggio 2026

Licenziare per l'AI: cosa è già lecito, cosa è ancora controverso e cosa manca

L'intelligenza artificiale sta entrando nei luoghi di lavoro come variabile organizzativa strutturale. Nel marzo 2026, le aziende americane hanno citato l'AI come causa di 15.341 tagli, pari al 25% dei licenziamenti annunciati nel mese. Le quattro grandi piattaforme tecnologiche, Amazon, Alphabet, Microsoft e Meta, hanno mandato a casa almeno 60.000 persone dall'inizio del 2025, in parallelo a investimenti previsti in AI per circa 650 miliardi di dollari entro fine 2026. Il diritto del lavoro, in Italia come in Europa, si trova a fare i conti con un fenomeno che le norme vigenti non avevano esplicitamente previsto, ma che gli strumenti esistenti stanno già cercando di governare.

La prima sentenza italiana: il licenziamento per AI può essere legittimo

Il Tribunale di Roma, con la sentenza n. 9135 del 19 novembre 2025, ha ritenuto legittimo il licenziamento di una graphic designer impiegata in una società di cybersecurity, nell'ambito di una riorganizzazione interna in cui l'uso di strumenti di AI ha contribuito a rendere superfluo il suo ruolo. La sentenza chiarisce che l'AI non è una causa autonoma di licenziamento, ma può incidere sull'organizzazione del lavoro.

"Il datore di lavoro che intende licenziare invocando l'automazione non è esonerato dagli obblighi ordinari"

Il giudice ha applicato il classico schema del giustificato motivo oggettivo, valutando la genuinità della riorganizzazione aziendale e l'assolvimento dell'obbligo di repêchage, cioè la verifica che non esistessero mansioni alternative da assegnare alla lavoratrice. Il punto è rilevante: il datore di lavoro che intende licenziare invocando l'automazione non è esonerato dagli obblighi ordinari. Deve dimostrare che la riorganizzazione è reale, che la posizione soppressa non è sostituibile con altra, e che ha esplorato soluzioni alternative prima di procedere al licenziamento.

Licenziare per l'AI: cosa è già lecito, cosa è ancora controverso e cosa manca

Il quadro normativo europeo: obblighi di trasparenza e diritti sindacali
L'AI Act europeo, nei settori occupazione, gestione dei lavoratori e accesso al lavoro, include i sistemi AI tra le aree ad alto rischio, con obblighi rafforzati di documentazione, supervisione umana e trasparenza. Per i datori di lavoro che adottano sistemi AI per valutare performance, assegnare turni, selezionare candidati o monitorare produttività, questi obblighi sono già operativi o in via di applicazione. Il quadro normativo italiano si completa con lo Statuto dei Lavoratori (in particolare l'art. 4 sul controllo a distanza) con il GDPR in tema di tutela dei dati personali e con gli accordi collettivi che introducono obblighi di informazione specifica sulle caratteristiche tecniche dei sistemi AI utilizzati, nonché un parallelo diritto di accesso in favore del lavoratore e delle rappresentanze sindacali. Chi adotta sistemi di AI nei processi di gestione del personale deve fornire informazioni adeguate prima ancora che il sistema produca effetti sul rapporto di lavoro.

La differenza tra USA e Europa
Il divario tra i due sistemi è strutturale. Negli Stati Uniti non esiste una norma federale che imponga al datore di lavoro di giustificare la scelta di automatizzare, né obblighi di consultazione sindacale in caso di riorganizzazione tecnologica. L'amministrazione Trump ha scelto la strada di lasciare i protagonisti dell'AI senza vincoli regolatori, con la scusa di dover vincere la corsa tecnologica contro la Cina. Il risultato è che la tutela del lavoratore dipende quasi interamente dalla contrattazione collettiva e dalla capacità dei sindacati di negoziare clausole specifiche. In Europa, e in Italia in particolare, il sistema è più vincolante: la riorganizzazione che coinvolge l'AI non esime il datore dagli obblighi procedurali del licenziamento collettivo, dall'obbligo di informazione e consultazione sindacale, né dalla verifica del repêchage nel licenziamento individuale.

Cosa manca ancora
Le leggi e i contratti collettivi prevedono strumenti di controllo e consultazione che diventano fondamentali in questo contesto. La sfida è renderli effettivi: occorre che le organizzazioni sindacali compiano un processo di digitalizzazione, affinché gli strumenti a disposizione vengano realmente compresi e sfruttati senza rimanere solo mezzi di tutela su carta. Il diritto del lavoro italiano dispone degli strumenti per governare i licenziamenti da AI. Il problema non è normativo: è applicativo. E la giurisprudenza, con la sentenza di Roma, ha iniziato a costruire i primi mattoni di un orientamento che sarà inevitabilmente destinato a crescere.

Allinea
Avvera Compliance Review
Maggio 2026

L'AI accelera il crimine informatico: cosa dice l'IOCTA 2026 di Europol e cosa devono fare le imprese

Il 28 aprile 2026 Europol ha pubblicato la nuova edizione dell'Internet Organised Crime Threat Assessment, il rapporto annuale sulle principali minacce del crimine informatico nell'Unione Europea. Il titolo scelto – "How encryption, proxies, and AI are expanding cybercrime"- è già una sintesi del messaggio centrale: l'intelligenza artificiale, la crittografia end-to-end e le infrastrutture anonimizzate hanno ampliato la capacità operativa delle reti criminali in modo strutturale, non episodico.

Il velocity gap: i criminali corrono più veloci delle forze dell'ordine

Il concetto chiave introdotto dal rapporto è quello di "velocity gap": i criminali informatici stanno guadagnando terreno sulle forze dell'ordine a un ritmo senza precedenti. Mentre le autorità operano all'interno di framework giuridici che richiedono raccolta di prove, cooperazione internazionale e rispetto del giusto processo, i criminali sfruttano comunicazioni cifrate, tecnologie di anonimizzazione e confini giurisdizionali per agire in modo molto più rapido. Il velocity gap non riguarda solo la velocità degli attacchi, ma la loro scala e personalizzazione. I criminali integrano automazione e intelligenza artificiale per aumentare l'efficienza e la portata delle loro attività. Gli strumenti di AI generativa vengono usati per personalizzare le tattiche di social engineering, accelerando e occultando le frodi online. Il caller ID spoofing e le SIM farm (capaci di distribuire migliaia di SMS, chiamate e post sui social media) sono diventati facilitatori di frodi su larga scala.

Il ransomware si trasforma: dalla cifratura all'estorsione pura

Il ransomware rimane la minaccia dominante nell'UE, con oltre 120 brand attivi rilevati da Europol nel 2025. Il modello estorsivo si sta spostando dalla cifratura dei dati al furto puro: gli attaccanti fanno sempre meno affidamento sul blocco dei sistemi e sempre più sulla minaccia di esporre i dati sottratti per forzare il pagamento. Un cambiamento che rende le misure di backup, tradizionalmente la principale difesa contro il ransomware, insufficienti da sole. La relazione tra attori di minaccia ibridi, strutture collegate a Stati, e criminali informatici si sta opacizzando. Gli attori ibridi usano reti criminali come proxy per operazioni destabilizzanti, inclusi attacchi DDoS, intrusioni e ransomware. Nel modello CaaS (Cybercrime as a Service) gli attori ibridi sono semplicemente un altro cliente.

Le implicazioni per le imprese europee

Il rapporto non è destinato solo alle forze dell'ordine. Per le imprese che operano nel mercato europeo, l'IOCTA 2026 fornisce un quadro di rischio che ha dirette implicazioni in termini di compliance. Sul fronte NIS2, il rapporto descrive esattamente la tipologia di minacce che la Direttiva, recepita in Italia con il D.Lgs. 138/2024, intende presidiare. Le misure di sicurezza che i soggetti NIS devono adottare entro il 31 luglio 2027 non sono adempimenti astratti: corrispondono alle minacce concrete che Europol documenta. La gestione del rischio nella catena di fornitura, il monitoraggio degli incidenti, la risposta agli attacchi ransomware e la protezione dei dati sono i quattro assi su cui il velocity gap si misura anche all'interno delle organizzazioni private. Sul fronte GDPR, la combinazione di AI generativa e social engineering produce violazioni dei dati personali sempre più difficili da rilevare in tempo utile. I criminali usano strumenti AI per personalizzare le frodi, accelerandole e occultandole.

L'AI accelera il crimine informatico: cosa dice l'IOCTA 2026 di Europol e cosa devono fare le imprese

Questo aumenta il rischio che le organizzazioni non si accorgano di una violazione entro le 72 ore previste dall'art. 33 del Regolamento, con le conseguenze sanzionatorie che ne derivano.

Cosa fare adesso
Il velocity gap descritto da Europol non è colmabile solo con investimenti tecnologici. Richiede processi: procedure di incident response documentate e testate, sistemi di monitoraggio continuo, formazione del personale sulle tecniche di social engineering potenziate dall'AI, e una governance della sicurezza che coinvolga il vertice aziendale, non solo il reparto IT. Le imprese che ancora trattano la cybersecurity come un problema tecnico e non come un rischio di business con implicazioni legali dirette stanno già correndo in ritardo.

Allinea
Avvera Compliance Review
Maggio 2026

Agenti AI e harness: chi risponde quando la macchina decide?

Nel 2026 il vero prodotto degli ecosistemi agentici non è il modello di linguaggio. È l'harness: l'infrastruttura software che avvolge il modello, ne governa il comportamento e trasforma la sua capacità cognitiva grezza in lavoro eseguibile. Retrieval, memoria, tool dispatch, orchestrazione, safety enforcement, observability sono questi i sei layer che determinano cosa un agente fa davvero, con quali dati, con quali limiti, con quale traccia lasciata. Questa distinzione, già consolidata nella letteratura tecnica, non ha ancora trovato un corrispondente quadro giuridico adeguato. Ed è esattamente qui che si concentrano i problemi di responsabilità più rilevanti del prossimo ciclo regolatorio.

Il modello è una commodity. La responsabilità no.
L'AI Act costruisce la sua architettura su due figure: il provider (chi mette a disposizione il sistema) e il deployer (chi lo usa in contesto operativo). Ma lo stack agentico reale è molto più articolato. Tra il fondatore del modello (Anthropic, OpenAI, Google), il costruttore dell'harness, l'integratore di dominio che assembla i tool proprietari e l'utilizzatore finale, la catena della responsabilità si distribuisce su quattro livelli che il testo normativo non contempla esplicitamente. La risposta attuale a "chi risponde quando l'agente sbaglia?" è: dipende dai contratti. E i contratti B2B del settore tendono sistematicamente a scaricare il rischio verso il basso della filiera, verso chi ha minori capacità di compliance.

"Un sistema con observability sottosviluppata non è solo inefficiente - in molti contesti regolamentati, è non conforme"

Il dato che avvelena la catena.
Un dato McKinsey del 2026 sposta il baricentro del problema in modo inaspettato: l'80% del tempo di implementazione dell'AI agentiva viene consumato da data engineering e governance, non dalla configurazione dei framework. E gran parte di ciò che viene liquidato come allucinazione degli LLM è in realtà conseguenza di fonti di dati inconsistenti, obsolete o parzialmente replicate. L'OWASP Top 10 per le applicazioni agentive identifica il memory poisoning e i cascading failures tra i rischi più critici, entrambi causati da input corrotti che entrano nel contesto dell'harness. Dal punto di vista del diritto della responsabilità, questo configura un nesso causale nuovo: non sbaglia il modello, non malfunziona l'harness, ma è il dato che contamina l'intera catena decisionale. Il principio di accuratezza del GDPR (art. 5, par. 1, lett. d) non è stato pensato per ecosistemi dove lo stesso dato viene recuperato, compresso, memorizzato e citato come fonte in sessioni successive. Una reinterpretazione operativa è urgente.

Agenti AI e harness: chi risponde quando la macchina decide?

Observability: da KPI tecnico a condizione di legittimità.
La letteratura tecnica tratta l'observability come indicatore di maturità operativa. Giuridicamente è qualcosa di più: è una condizione di legittimità. L'AI Act impone la tenuta di log per i sistemi ad alto rischio (art. 12). Il GDPR impone la capacità di rispondere alle richieste degli interessati sulle decisioni automatizzate (art. 22). NIS2 impone la ricostruzione documentabile degli incidenti. Tutti e tre i corpi normativi presuppongono un livello di tracciabilità che, nell'ecosistema agentico attuale, non è garantito di default: dipende da una scelta architetturale precisa, cioè da come è costruito l'harness. Un sistema con observability sottosviluppata non è solo inefficiente - in molti contesti regolamentati, è non conforme.

La tesi: l'harness è il nuovo titolare del trattamento.
La conclusione operativa è questa: l'harness è funzionalmente equivalente al titolare del trattamento nel senso del GDPR - non per analogia letterale, ma perché è il layer che determina le finalità e i mezzi con cui il modello opera. Chi progetta e controlla l'harness esercita il potere decisionale effettivo sull'agente. Il fornitore del modello sottostante è più assimilabile a un responsabile del trattamento: elabora dati per conto del titolare, secondo istruzioni definite. Chi costruisce le integrazioni proprietarie - tool di dominio, dataset di valutazione, environment map - porta la responsabilità operativa maggiore, spesso senza averne piena consapevolezza contrattuale. Prima di ogni deployment la domanda non è quale modello scegliere. È: chi controlla l'harness, con quale governance, con quale audit trail, con quale contratto di responsabilità verso tutti gli stakeholder coinvolti? Le aziende che hanno capito questo stanno investendo nell'infrastruttura di controllo ora. Le altre scopriranno il problema quando il contenzioso sarà già aperto.

Allinea

Avvera Compliance Review

Newsletter Informativa
riservata a clienti e partner
di Avvera

Maggio

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