FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 15/2026

DATA PROTECTION

29 Luglio 2026 – Garante privacy: e-mail aziendali e controlli difensivi, sanzione di 460.000 euro a Piaggio per la conservazione sistematica della posta elettronica dei dipendenti.

---

28 Luglio 2026 – Web scraping e risarcimento collettivo: il Tribunale di Milano ammette l'azione rappresentativa privacy contro Meta.

INTELLIGENZA ARTIFICIALE

30 Luglio 2026 - AI Act, dal 2 agosto scattano gli obblighi di trasparenza. La Commissione UE aggiorna le proprie FAQ sull'articolo 50 dell'AI Act, ad integrazione delle Linee guida definitive pubblicate il 20 luglio 2026.

---

29 Luglio 2026 – Garante privacy; parere favorevole allo schema di decreto legislativo che coordina la normativa italiana all'AI Act.

---

29 Luglio 2026 – Garante privacy: parere favorevole allo schema di decreto legislativo su riconoscimento facciale e IA nelle attività di polizia. Vietate le raccolte biometriche massive e banche dati create mediante scraping.

---

27 Luglio 2026 – In vigore il Regolamento 2026/1744 (Digital Omnibus sull'IA): più tempo per i sistemi ad alto rischio, meno oneri per le imprese e nuovi poteri all'AI Office.

---

22 Luglio 2026 – Banca d'Italia e IVASS: entro il 31 dicembre 2026 banche e assicurazioni dovranno presentare un piano sui nuovi rischi cyber dell'IA.

CYBERSICUREZZA

27 Luglio 2026 – Commissione UE: pubblicata una guida operativa per le imprese sul Cyber Resilience Act.

---

24 Luglio 2026 – Agenzia nazionale per la cybersicurezza: aggiornate le FAQ sulle misure di sicurezza per la supply chain dei soggetti NIS.

MERCATI DIGITALI

28 Luglio 2026 – La Francia è il primo Paese dell'UE a vietare i social network ai minori di 15 anni.

---

22 Luglio 2026 – Corte di Giustizia UE: Google può essere ritenuta responsabile per i video YouTube di un creatore di contenuti vincolato da una partnership commerciale.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

25 Luglio 2026 – Organizzazione Mondiale della Proprietà Intellettuale: nel 2025 superata per la prima volta la barriera dei 10.000 miliardi di dollari in investimenti per beni immateriali.

DATA PROTECTION

29 Luglio 2026 – Garante privacy: e-mail aziendali e controlli difensivi, sanzione di 460.000 euro a Piaggio per la conservazione sistematica della posta elettronica dei dipendenti.

Il Garante per la protezione dei dati personali ha sanzionato Piaggio & C. S.p.A. per 460.000 euro, dichiarando illecito il trattamento dei dati relativi alla posta elettronica aziendale dei dipendenti e vietando alla società di accedere ai contenuti raccolti e conservati nei propri sistemi. L'istruttoria, avviata a seguito dei reclami di due ex dipendenti, ha accertato che la società aveva acquisito complessivamente 112 messaggi di posta elettronica — 18 relativi a una lavoratrice e 94 a un lavoratore — per verificare la fondatezza di sospetti riguardanti presunte condotte illecite. La ricerca era stata effettuata anche su comunicazioni risalenti a circa due anni prima dell'insorgenza del sospetto e aveva interessato messaggi transitati attraverso caselle aziendali e, in alcuni casi, corrispondenza con account personali e soggetti terzi.

Il Garante ha richiamato la giurisprudenza della Corte di cassazione secondo cui i controlli tecnologici diretti a tutelare il patrimonio aziendale o ad accertare comportamenti illeciti possono essere ammessi, in presenza di un fondato sospetto, soltanto nel rispetto di un adeguato bilanciamento con la dignità e la riservatezza del lavoratore. Un punto è però decisivo: il controllo difensivo deve riguardare dati acquisiti successivamente alla nascita del sospetto. Non può quindi essere utilizzato per legittimare ricerche retrospettive su una massa di comunicazioni raccolte sistematicamente prima che emergessero elementi concreti di possibile illecito. Nel caso esaminato, la ricerca era stata invece estesa a ritroso sino a circa due anni prima.

La predisposizione di una procedura interna, di parole chiave, di filtri di ricerca o di un test di bilanciamento non è quindi, da sola, sufficiente a rendere lecito l'accesso alla posta elettronica. Occorre anzitutto verificare che i dati siano stati raccolti e conservati legittimamente e che il controllo rispetti i limiti temporali e sostanziali stabiliti dalla disciplina lavoristica e dalla giurisprudenza. L'attività di indagine era stata resa possibile da un sistema che prevedeva il backup della posta elettronica per tutta la durata del rapporto di lavoro e sino a cinque anni dopo la sua cessazione, oltre alla conservazione dei log della posta per sei mesi. Secondo il Garante, la raccolta sistematica di e-mail e metadati per periodi così estesi consentiva di ricostruire l'attività dei dipendenti e rendeva possibile un controllo a distanza in assenza delle garanzie previste dall'articolo 4 dello Statuto dei lavoratori, richiamato dall'articolo 114 del Codice privacy. Il trattamento è stato pertanto ritenuto contrario ai principi di liceità, limitazione delle finalità, minimizzazione e limitazione della conservazione previsti dal GDPR. L'Autorità ha inoltre ribadito che gli archivi di posta devono essere protetti mediante misure organizzative e tecnologiche che impediscano l'accesso da parte di soggetti diversi dall'intestatario, salvo una sua espressa richiesta per finalità di assistenza.

Ulteriori violazioni hanno riguardato la trasparenza. Le policy aziendali non indicavano in modo sufficientemente preciso le finalità e i presupposti giuridici della conservazione delle e-mail e dei relativi log. La sola indicazione dei periodi di conservazione non è sufficiente: i lavoratori devono essere informati preventivamente e in maniera comprensibile anche sulle ragioni del trattamento, sulle basi giuridiche e sulle concrete modalità degli eventuali controlli.

La società non aveva inoltre risposto alle richieste con cui gli ex dipendenti chiedevano conferma della disattivazione dei propri account individuali. Il Garante ha chiarito che una simile richiesta costituisce esercizio dei diritti riconosciuti dal GDPR, anche quando l'interessato non richiami espressamente una specifica disposizione normativa.

Il provvedimento impone alle aziende di riesaminare non soltanto le procedure di accesso alla posta elettronica, ma l'intera architettura di raccolta e conservazione dei dati generati dagli strumenti di lavoro.

La decisione conferma che il controllo difensivo non può sanare una raccolta preventiva, generalizzata e sproporzionata della corrispondenza. Per le imprese, la gestione della posta elettronica aziendale deve essere progettata sin dall'origine secondo i principi di minimizzazione, privacy by design e accountability, evitando di creare archivi che consentano una ricostruzione indiscriminata dell'attività lavorativa.

28 Luglio 2026 – Web scraping e risarcimento collettivo: il Tribunale di Milano ammette l'azione rappresentativa privacy contro Meta.

Il Tribunale di Milano, Sezione XIV civile – Sezione specializzata in materia di impresa "A", n. 1251/2026 ha dichiarato ammissibile l'azione rappresentativa proposta da un'associazione di consumatori nei confronti di Meta, diretta a ottenere il risarcimento dei danni che gli utenti di Facebook avrebbero subito a causa di una raccolta massiva di dati personali effettuata da terzi mediante tecniche di *web scraping*.

La decisione riguarda, in questa fase, esclusivamente l'ammissibilità dell'azione. L'effettiva responsabilità di Meta e la sussistenza dei danni lamentati dovranno essere accertate nel successivo giudizio di merito. Secondo la prospettazione accolta ai fini dell'ammissibilità, la responsabilità della piattaforma potrebbe derivare dall'insufficienza delle misure tecniche e organizzative adottate per impedire o limitare l'estrazione non autorizzata dei dati degli utenti. La contestazione coinvolge, pertanto, non soltanto gli obblighi di sicurezza previsti dal GDPR, ma anche i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'articolo 25 del Regolamento.

L'ordinanza del Tribunale di Milano rappresenta uno dei primi significativi punti di incontro, nella giurisprudenza italiana, tra il regime della responsabilità previsto dal GDPR e la disciplina delle azioni rappresentative dei consumatori. Il tema assume particolare rilievo anche alla luce delle recenti *Linee guida 03/2026 sul web scraping nel contesto dell'intelligenza artificiale generativa*, che richiamano la necessità di valutare i rischi connessi alla disponibilità online dei dati personali e di predisporre misure adeguate contro attività automatizzate di raccolta massiva. Sul medesimo episodio, Meta era già stata destinataria di un provvedimento sanzionatorio della Data Protection Commission irlandese.

L'ordinanza presenta almeno tre profili di particolare interesse. In primo luogo, il Tribunale ha riconosciuto la legittimazione dell'associazione dei consumatori ad agire senza necessità di ottenere preventivamente uno specifico mandato da ciascun interessato. La conclusione è fondata sulla funzione propria dell'azione rappresentativa, destinata a garantire una tutela effettiva e di livello elevato agli interessi collettivi dei consumatori. In secondo luogo, la decisione si colloca nel solco della giurisprudenza della Corte di giustizia dell'Unione europea sul risarcimento del danno da violazione del GDPR. La perdita del controllo sui propri dati personali può integrare un danno non patrimoniale risarcibile senza che sia necessario dimostrare il superamento di una soglia minima di gravità o di tollerabilità. Rimane comunque necessario accertare, per ciascuna categoria di soggetti, l'esistenza concreta del danno e il nesso causale con la violazione contestata. Infine, il requisito dell'omogeneità dei diritti azionati collettivamente può sussistere anche quando il medesimo comportamento produca conseguenze dannose differenti. È possibile individuare sottoclassi di utenti interessate da specifiche tipologie di pregiudizio, purché i relativi danni possano essere valutati attraverso criteri sufficientemente uniformi e standardizzabili.

La pronuncia amplia sensibilmente la dimensione del rischio connesso alle violazioni della normativa sulla protezione dei dati personali. Alle sanzioni amministrative e ai possibili provvedimenti correttivi delle autorità di controllo può infatti aggiungersi una responsabilità civile esercitata in forma collettiva, con effetti economici, reputazionali e organizzativi potenzialmente molto rilevanti.
Il rischio non riguarda soltanto le grandi piattaforme digitali. Può coinvolgere qualsiasi impresa che renda disponibili online dati personali, gestisca portali o aree riservate, utilizzi interfacce di programmazione, esponga database accessibili dall'esterno o tratti grandi quantità di informazioni suscettibili di estrazione automatizzata.

Alla luce della decisione, le organizzazioni dovrebbero:

1. valutare specificamente il rischio di scraping nell'ambito delle analisi di sicurezza e delle valutazioni d'impatto;
2. verificare se siti, piattaforme, API e applicazioni consentano interrogazioni automatizzate o estrazioni massive di dati;
3. adottare misure proporzionate, quali limitazioni delle richieste, controlli sugli accessi, sistemi di rilevazione delle anomalie e meccanismi anti-bot;
4. applicare concretamente i principi di privacy by design e by default, limitando i dati visibili e accessibili a quanto strettamente necessario;

5. definire procedure per individuare, contenere e documentare tempestivamente eventuali attività di raccolta non autorizzata;
6. riesaminare informative, condizioni d'uso, accordi con fornitori tecnologici e attribuzione delle responsabilità lungo la catena dei trattamenti;
7. conservare evidenza delle valutazioni effettuate, delle misure implementate, dei test svolti e delle decisioni assunte;
8. considerare, nella quantificazione del rischio privacy, anche la possibile esposizione ad azioni risarcitorie rappresentative.

INTELLIGENZA ARTIFICIALE

30 Luglio 2026 - AI Act, dal 2 agosto scattano gli obblighi di trasparenza. La Commissione UE aggiorna le proprie FAQ sull'articolo 50 dell'AI Act, ad integrazione delle Linee guida definitive pubblicate il 20 luglio 2026.

La Commissione europea ha aggiornato le proprie FAQ sull'articolo 50 dell'AI Act, a integrazione delle Linee guida definitive pubblicate il 20 luglio 2026. I chiarimenti precisano quali imprese debbano informare gli utenti dell'impiego dell'intelligenza artificiale e come debbano essere marcati o etichettati i contenuti generati o manipolati artificialmente. Gli obblighi si applicano dal 2 agosto 2026.

I provider devono progettare i sistemi destinati a interagire direttamente con persone fisiche in modo che l'utente sia informato di stare comunicando con un sistema di IA. L'avviso non è necessario soltanto quando la natura artificiale dell'interazione risulti evidente, eccezione che deve essere valutata restrittivamente in relazione al contesto concreto.

I provider di sistemi generativi, compresi i sistemi di IA per finalità generali, devono inoltre fare in modo che gli output audio, immagini, video e testi siano:

- marcati in un formato leggibile da macchina;
- riconoscibili come generati o manipolati mediante IA;
- supportati da soluzioni tecniche efficaci, interoperabili, robuste e affidabili, nei limiti della fattibilità tecnica e dello stato dell'arte.

I deployer, ossia le organizzazioni che utilizzano sistemi di IA sotto la propria autorità per finalità professionali, devono informare le persone esposte a sistemi di riconoscimento delle emozioni o di categorizzazione biometrica.

Devono inoltre rendere riconoscibili:

- immagini, audio o video che costituiscono un *deepfake*;
- testi generati o manipolati mediante IA e pubblicati allo scopo di informare il pubblico su questioni di interesse pubblico.

Per questi ultimi testi, l'obbligo non si applica quando il contenuto sia stato sottoposto a revisione umana o controllo editoriale e una persona fisica o giuridica ne abbia assunto la responsabilità editoriale. L'esenzione non può quindi essere invocata sulla base di una verifica meramente formale o automatizzata.

Per le opere manifestamente artistiche, creative, satiriche o fittizie contenenti deepfake, l'informazione deve essere fornita in modo appropriato, senza compromettere la fruizione dell'opera. Restano inoltre le specifiche deroghe per gli utilizzi autorizzati dalla legge a fini di prevenzione, accertamento, indagine o perseguimento dei reati.

La Commissione chiarisce anche che, quando il sistema è utilizzato nell'ambito dell'organizzazione, il deployer è normalmente la persona giuridica. Dipendenti, collaboratori e freelance che operano sotto le sue istruzioni, responsabilità e controllo non assumono autonomamente tale qualifica.

La proroga al 2 dicembre 2026 non riguarda tutti gli obblighi dell'articolo 50. Essa si applica esclusivamente alla marcatura e rilevabilità dei contenuti prevista dall'articolo 50, paragrafo 2, per i sistemi già immessi sul mercato o messi in servizio prima del 2 agosto 2026.

Gli altri obblighi — compresi gli avvisi sull'interazione con l'IA, sui sistemi biometrici e di riconoscimento delle emozioni e l'etichettatura dei deepfake — si applicano dal 2 agosto 2026. I contenuti già generati e resi disponibili prima di tale data non devono invece essere etichettati retroattivamente.

Provider e deployer dovrebbero:

1. censire chatbot, assistenti virtuali, agenti, sistemi generativi e strumenti biometrici utilizzati;
2. qualificare correttamente il ruolo dell'impresa per ciascun sistema;
3. introdurre avvisi chiari e accessibili prima o al momento dell'interazione con l'IA;
4. verificare con i fornitori la disponibilità di marcature leggibili da macchina e strumenti di rilevazione;
5. definire procedure per etichettare deepfake e contenuti di interesse pubblico;
6. documentare l'eventuale revisione umana e l'effettiva assunzione della responsabilità editoriale;
7. aggiornare contratti, policy editoriali, procedure di pubblicazione e istruzioni al personale;
8. conservare evidenza delle valutazioni e delle soluzioni adottate per dimostrare la conformità.

Il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA costituisce uno strumento volontario riconosciuto dalla Commissione e dall'AI Board per facilitare la conformità agli obblighi di marcatura ed etichettatura. L'adesione non prova automaticamente il rispetto dell'AI Act, mentre le imprese che non aderiscono devono essere in grado di dimostrare attraverso misure alternative adeguate la conformità delle proprie procedure.

---

29 Luglio 2026 – Garante privacy; parere favorevole allo schema di decreto legislativo che coordina la normativa italiana all'AI Act.

Il Garante per la protezione dei dati personali ha espresso parere favorevole, con condizioni e osservazioni, sullo schema di decreto legislativo destinato ad adeguare l'ordinamento italiano all'AI Act in materia di autorità competenti, vigilanza del mercato, sperimentazione e formazione. Il parere, n. 532 del 14 luglio 2026, riguarda l'Atto del Governo n. 421, approvato in via preliminare dal Consiglio dei ministri il 10 giugno 2026 e successivamente trasmesso alle Camere: il testo non costituisce, pertanto, ancora il decreto legislativo definitivo.

Lo schema individua nell'AgID e nell'Agenzia per la cybersicurezza nazionale – ACN le autorità nazionali per l'intelligenza artificiale. AgID svolgerà le funzioni di autorità di notifica degli organismi incaricati delle valutazioni di conformità, mentre l'ACN assumerà il ruolo generale di autorità di vigilanza del mercato.

Competenze specifiche sono attribuite alla Banca d'Italia, alla Consob e all'IVASS per i sistemi di IA impiegati nei rispettivi settori finanziari, bancari, creditizi e assicurativi. Il Garante sarà invece autorità di vigilanza per i sistemi ad alto rischio utilizzati negli ambiti particolarmente sensibili indicati dall'articolo 74, paragrafo 8, dell'AI Act, tra cui attività di contrasto, gestione delle frontiere e dell'immigrazione, amministrazione della giustizia e processi democratici.

Lo schema disciplina inoltre lo Spazio di sperimentazione italiano per l'IA, gestito congiuntamente da AgID e ACN, nel quale provider e sviluppatori potranno sperimentare sistemi di intelligenza artificiale in un ambiente controllato. Sono previste anche misure per la formazione nelle scuole, nelle università e nei percorsi professionali, con particolare attenzione all'uso consapevole dell'IA, alla tutela dei dati personali, alla sicurezza e alla non discriminazione.

Pur giudicando lo schema complessivamente coerente con l'AI Act e con la legge italiana n. 132/2025, il Garante ha richiesto alcune integrazioni. In primo luogo, l'Autorità chiede che anche al Garante, e non soltanto ad AgID, ACN e alle autorità finanziarie, sia espressamente riconosciuto il potere di adottare linee guida, raccomandazioni e buone pratiche. Tale competenza è ritenuta necessaria per assicurare un'applicazione uniforme delle regole nei settori nei quali l'utilizzo dell'IA incide direttamente sulla protezione dei dati e sugli altri diritti fondamentali.

Il decreto dovrebbe inoltre precisare che i procedimenti sanzionatori di competenza del Garante saranno regolati dall'articolo 166 del Codice privacy, chiarendo anche la destinazione dei proventi derivanti dalle sanzioni.
Un ulteriore intervento è richiesto in materia di valutazione della conformità. Poiché l'AI Act attribuisce al Garante specifiche funzioni rispetto ai sistemi ad alto rischio rientranti nella sua competenza, il legislatore dovrà chiarire se lo Stato assumerà direttamente la responsabilità delle relative attività di valutazione oppure se dovrà trovare applicazione il diverso regime assicurativo previsto dal Regolamento europeo.

Lo schema affida la gestione dello Spazio di sperimentazione italiano ad AgID e ACN, ma non prevede espressamente la partecipazione del Garante ai progetti che comportano trattamenti di dati personali. Secondo l'Autorità, questa omissione deve essere corretta: l'articolo 57, paragrafo 10, dell'AI Act richiede infatti il coinvolgimento delle autorità di protezione dei dati quando le attività svolte all'interno di una sandbox comprendono trattamenti soggetti al GDPR. Il confronto con il Garante dovrà quindi intervenire sin dalla progettazione della sperimentazione e non soltanto dopo l'emersione di eventuali criticità.

Particolare attenzione è dedicata all'impiego dell'intelligenza artificiale nei rapporti di lavoro. Lo schema stabilisce che le decisioni sulla costituzione, modifica o cessazione del rapporto non possano essere adottate esclusivamente attraverso un trattamento automatizzato e che la decisione finale debba spettare a una persona dotata di effettiva autonomia.
Il Garante propone di estendere questa garanzia anche alle decisioni valutative suscettibili di incidere significativamente sul rapporto di lavoro, come quelle relative alla misurazione delle prestazioni, all'attribuzione di premi, alla classificazione professionale e alle progressioni di carriera.
Il datore di lavoro dovrà inoltre informare preventivamente i lavoratori, rispettare dignità, riservatezza e non discriminazione e assicurare una motivazione comprensibile delle decisioni, indicando il ruolo svolto dal sistema di IA e i principali parametri utilizzati.

---

29 Luglio 2026 – Garante privacy: parere favorevole allo schema di decreto legislativo su riconoscimento facciale e IA nelle attività di polizia. Vietate le raccolte biometriche massive e banche dati create mediante scraping.

Il Garante per la protezione dei dati personali ha espresso parere favorevole con condizioni sullo schema di decreto legislativo che disciplina l'utilizzo dei sistemi di intelligenza artificiale da parte delle Forze di polizia, compreso il ricorso all'identificazione biometrica remota in tempo reale e al riconoscimento facciale a posteriori.
Il parere n. 531 del 14 luglio 2026 riguarda l'Atto del Governo n. 418, adottato in attuazione della delega contenuta nella legge 23 settembre 2025, n. 132. Lo schema dovrà ancora completare il proprio iter e non costituisce, quindi, il testo definitivo della disciplina nazionale.

Lo schema consente alle Forze di polizia di utilizzare sistemi di identificazione biometrica remota in tempo reale, in luoghi pubblici o aperti al pubblico, soltanto nelle ipotesi eccezionali ammesse dall'AI Act: prevenzione di specifiche minacce, ricerca di persone scomparse o di vittime di determinati reati e, nell'ambito delle indagini penali, ricerca mirata di persone specificamente individuate o individuabili.
L'impiego deve essere autorizzato dall'autorità giudiziaria, riferito a uno specifico evento, limitato a un'area territoriale e a un periodo determinati e basato su una banca dati di confronto adeguata alla concreta finalità perseguita. In caso di urgenza è prevista una procedura accelerata, sottoposta a successiva convalida. Il mancato rispetto dei presupposti e dei termini comporta l'inutilizzabilità dei risultati e, in linea di principio, la cancellazione dei dati acquisiti.

Uno dei principali rilievi dell'Autorità riguarda la qualità e la composizione delle banche dati biometriche impiegate per il confronto.
Secondo il Garante, il decreto deve stabilire requisiti specifici per ridurre il rischio di falsi positivi, errori di identificazione e risultati discriminatori. Occorre inoltre chiarire se la banca dati debba essere costituita appositamente per ciascuna operazione oppure possa avere carattere stabile.
Anche in quest'ultimo caso, il set di confronto dovrà contenere soltanto i dati pertinenti alla singola ricerca autorizzata e non potrà ampliarsi progressivamente accumulando i dati utilizzati nelle operazioni precedenti. Dovranno essere disciplinati anche misure di sicurezza, tempi di conservazione, modalità di cancellazione e garanzie contro l'incremento indiscriminato dell'archivio.

Il Garante chiede inoltre di circoscrivere rigorosamente le eccezioni all'obbligo di cancellare i dati acquisiti illegittimamente. Il generico richiamo alla possibilità di conservarli sulla base di un diverso titolo giuridico rischierebbe, infatti, di svuotare le garanzie previste dal decreto legislativo n. 51/2018 per i trattamenti effettuati a fini di polizia.

Particolarmente rilevante è la posizione dell'Autorità sul riconoscimento facciale a posteriori applicato alle immagini raccolte mediante videosorveglianza.
Lo schema sembrava consentire la preventiva elaborazione e memorizzazione dei dati biometrici di tutte le persone che accedono a luoghi o eventi interessati da esigenze di ordine e sicurezza pubblica, come stadi, concerti, manifestazioni, stazioni o grandi eventi.
Per il Garante, una simile raccolta automatizzata e generalizzata non è compatibile con l'AI Act. Il riconoscimento facciale a posteriori può essere utilizzato soltanto per una ricerca mirata ex post, riguardante persone sospettate o condannate per un reato.
La trasformazione delle immagini in modelli biometrici non dovrebbe quindi avvenire automaticamente al momento della ripresa. L'elaborazione dovrebbe essere attivata soltanto sulle registrazioni già acquisite, quando sia emersa una specifica esigenza operativa connessa a un reato.

Lo schema già vieta, per alcune attività preventive di polizia, l'utilizzo di banche dati biometriche alimentate mediante tecniche di scraping non mirato o costituite in violazione della normativa sulla protezione dei dati personali.
Il Garante chiede che lo stesso divieto sia espressamente inserito anche nel nuovo articolo 359-ter del codice di procedura penale, destinato a disciplinare l'identificazione biometrica remota nell'ambito delle indagini.
Non potranno quindi essere utilizzati, neppure per finalità investigative, archivi di immagini facciali creati raccogliendo indiscriminatamente fotografie da siti internet, social network o altre fonti online, né database formati attraverso trattamenti illeciti.

Il Garante chiede inoltre di sostituire nello schema il riferimento alla semplice "revisione umana qualificata" con il concetto più ampio di sorveglianza umana, utilizzato dall'articolo 14 dell'AI Act. La persona incaricata non deve limitarsi a verificare formalmente il risultato, ma deve poter comprendere il funzionamento del sistema, valutare criticamente l'output e impedirne o interromperne l'utilizzo quando necessario.
Nei progetti di ricerca e sperimentazione, l'Autorità propone di vietare non soltanto la condivisione, ma anche l'impiego di dati operativi sensibili, privilegiando dati sintetici oppure dati reali sottoposti a masking o pseudonimizzazione. Devono inoltre essere chiariti i ruoli privacy dei soggetti pubblici e privati coinvolti.
Il Garante dovrà infine essere associato al funzionamento delle sandbox regolamentari ogni volta che la sperimentazione comporti un trattamento di dati personali. Oltre alla valutazione d'impatto sui diritti fondamentali prevista dall'AI Act, dovrà essere effettuata anche la specifica valutazione d'impatto sulla protezione dei dati richiesta dal decreto legislativo n. 51/2018.

---

27 Luglio 2026 – In vigore il Regolamento 2026/1744 (Digital Omnibus sull'IA): più tempo per i sistemi ad alto rischio, meno oneri per le imprese e nuovi poteri all'AI Office.

Dal 27 luglio 2026 è in vigore il Regolamento (UE) 2026/1744, noto come *Digital Omnibus on AI*, che modifica l'AI Act con l'obiettivo di semplificarne l'attuazione, ridurre alcuni oneri amministrativi e favorire l'innovazione, senza diminuire le garanzie poste a tutela della sicurezza e dei diritti fondamentali.

La novità più rilevante riguarda il rinvio delle disposizioni sui sistemi di IA ad alto rischio:

- **dal 2 dicembre 2027** si applicheranno le regole relative ai sistemi individuati dall'articolo 6, paragrafo 2, e dall'Allegato III dell'AI Act, utilizzati, tra l'altro, in ambito biometrico, occupazionale, educativo, infrastrutturale, migratorio e nell'accesso a servizi essenziali;
- **dal 2 agosto 2028** si applicheranno le regole sui sistemi ad alto rischio incorporati in prodotti o componenti di sicurezza disciplinati dalla normativa europea elencata nell'Allegato I, quali macchine, giocattoli e ascensori.

Non si tratta, tuttavia, di un rinvio generale dell'AI Act. Restano ferme le disposizioni già applicabili e le ulteriori scadenze previste dal Regolamento. In particolare, i provider di sistemi, compresi quelli di IA per

finalità generali, che generano contenuti sintetici audio, immagini, video o testi e che siano stati immessi sul mercato prima del 2 agosto 2026 dovranno adeguarsi all'obbligo di marcatura previsto dall'articolo 50, paragrafo 2, entro il 2 dicembre 2026.

L'AI Omnibus introduce inoltre misure di proporzionalità per le PMI, le start-up e le *small mid-cap enterprises*, estendendo a queste ultime alcune agevolazioni precedentemente riservate alle PMI. Sono previste, tra l'altro, modalità semplificate per la documentazione tecnica, sistemi di gestione della qualità proporzionati alla dimensione dell'organizzazione e accesso prioritario alle sandbox regolamentari.

Viene modificato anche l'obbligo di alfabetizzazione in materia di IA. Provider e deployer non devono più garantire astrattamente il raggiungimento di uno specifico livello di competenza, ma devono adottare misure idonee a sostenere lo sviluppo delle conoscenze del personale e delle altre persone che utilizzano o gestiscono sistemi di IA per loro conto, tenendo conto delle competenze, del contesto di utilizzo e dei soggetti sui quali i sistemi producono effetti. L'obbligo non è quindi eliminato: le imprese devono continuare a prevedere formazione, istruzioni interne e misure organizzative documentabili.

Sono ampliate le opportunità di sperimentazione. Gli Stati membri dovranno rendere operativa almeno una sandbox nazionale entro il 2 agosto 2027, mentre l'AI Office potrà istituire una sandbox a livello dell'Unione. Viene inoltre estesa la possibilità di effettuare test in condizioni reali, nel rispetto delle garanzie previste dall'AI Act e della normativa sulla protezione dei dati personali.

Sul piano della tutela dei diritti fondamentali, il Regolamento:

- vieta, dal 2 dicembre 2026, i sistemi destinati a generare contenuti intimi o sessualmente espliciti non consensuali e materiale di abuso sessuale sui minori, comprese le cosiddette applicazioni di "nudificazione";
- consente, in via eccezionale e quando strettamente necessario, il trattamento di categorie particolari di dati personali per individuare e correggere bias, purché non sia possibile utilizzare efficacemente dati ordinari, sintetici o anonimizzati e siano adottate rigorose misure di sicurezza, limitazione degli accessi, documentazione e cancellazione.

Il Regolamento semplifica inoltre alcune informazioni richieste per la registrazione nella banca dati europea dei sistemi ritenuti esenti dalla classificazione ad alto rischio, chiarisce il coordinamento tra AI Act e normativa europea sulla sicurezza dei prodotti e razionalizza le procedure applicabili agli organismi di valutazione della conformità.

Vengono infine rafforzati i poteri dell'AI Office, competente in via esclusiva per la vigilanza su determinate categorie di sistemi basati su modelli di IA per finalità generali e sui sistemi integrati nelle piattaforme online e nei motori di ricerca di dimensioni molto grandi. L'AI Office potrà richiedere informazioni, svolgere indagini e ispezioni e imporre misure correttive e sanzionatorie.

Le attività da avviare nelle imprese.

L'estensione dei termini non giustifica la sospensione dei programmi di adeguamento. Provider e deployer dovrebbero:

1. aggiornare il censimento dei sistemi di IA sviluppati, acquistati o utilizzati;
2. verificare la classificazione di ciascun sistema e distinguere i casi dell'Allegato III da quelli collegati ai prodotti dell'Allegato I;
3. rivedere le roadmap di conformità alla luce delle nuove date del 2 dicembre 2027 e del 2 agosto 2028;
4. gestire separatamente gli obblighi già applicabili o non rinviati, in particolare quelli relativi alle pratiche vietate e alla trasparenza dei contenuti sintetici;
5. aggiornare i programmi di AI literacy, conservando evidenza della formazione, delle istruzioni e delle misure adottate;
6. verificare l'eventuale qualifica come PMI o small mid-cap e le semplificazioni concretamente utilizzabili;
7. riesaminare contratti con provider, sviluppatori e fornitori, chiarendo ruoli, documentazione, accesso alle informazioni e responsabilità lungo la catena del valore;

8. coordinare l'AI governance con GDPR, cybersecurity, normativa di prodotto e tutela della proprietà intellettuale;
9. valutare l'accesso alle sandbox regolamentari per progetti innovativi o sistemi ancora in fase di sviluppo.

L'AI Omnibus concede alle imprese più tempo e strumenti di conformità proporzionati, ma rafforza al contempo i controlli e la vigilanza europea. Il periodo aggiuntivo dovrebbe quindi essere utilizzato per costruire una governance dell'IA effettiva, documentata e integrata nei processi aziendali.

---

22 Luglio 2026 – Banca d'Italia e IVASS: entro il 31 dicembre 2026 banche e assicurazioni dovranno presentare un piano sui nuovi rischi cyber dell'IA.

Banca d'Italia e IVASS hanno pubblicato, il 17 luglio 2026, due comunicazioni parallele sulla resilienza operativa digitale e sui rischi derivanti dai modelli avanzati di intelligenza artificiale. Le Autorità chiedono agli intermediari finanziari direttamente vigilati e alle imprese assicurative di verificare con urgenza l'adeguatezza dei propri presidi di sicurezza e di predisporre una specifica relazione, accompagnata da un piano di intervento, da trasmettere alla rispettiva Autorità entro il 31 dicembre 2026.

L'iniziativa non introduce una nuova disciplina autonoma, ma traduce in precise aspettative di vigilanza gli obblighi già previsti dal Regolamento (UE) 2022/2554 sulla resilienza operativa digitale del settore finanziario – DORA, alla luce dell'evoluzione delle minacce informatiche abilitate dall'IA.

Banca d'Italia e IVASS richiamano in particolare la capacità dei modelli di ultima generazione di individuare vulnerabilità nei software e, contemporaneamente, generare le modalità tecniche per sfruttarle, in tempi molto brevi e senza la necessità di competenze specialistiche particolarmente elevate.

L'IA può quindi ridurre drasticamente l'intervallo tra la scoperta di una vulnerabilità e il suo sfruttamento, aumentando la probabilità di attacchi efficaci e ampliando l'asimmetria tra attaccanti e difensori. La resilienza digitale non viene perciò considerata soltanto un adempimento regolamentare, ma un presupposto della continuità operativa e dell'affidabilità dei servizi finanziari e assicurativi.

Le comunicazioni riguardano, per Banca d'Italia, le categorie di intermediari direttamente vigilati indicate nel documento, tra cui banche e gruppi bancari meno significativi, istituti di pagamento e di moneta elettronica, imprese di investimento, gestori, operatori in cripto-attività, fornitori di crowdfunding e intermediari finanziari. La comunicazione IVASS è invece rivolta alle imprese di assicurazione e riassicurazione con sede in Italia e alle rappresentanze italiane delle imprese aventi sede in uno Stato esterno allo Spazio economico europeo.

Le imprese devono effettuare una verifica strutturata in sei ambiti.

Il primo riguarda la governance. Gli organi di amministrazione e gestione devono aggiornare il Risk Appetite Framework per includere i rischi connessi alle tecnologie di frontiera, assegnare chiaramente le responsabilità, programmare investimenti ICT adeguati e assicurare la presenza di competenze tecnologiche e sull'intelligenza artificiale anche all'interno del consiglio di amministrazione.

Particolare rilievo assume la gestione dei fornitori ICT: selezione preventiva, monitoraggio continuo, obblighi contrattuali sulla sicurezza e tempi di applicazione delle patch devono essere adeguati al nuovo scenario di rischio.

Le altre aree riguardano:

1. igiene informatica e difesa in profondità, attraverso autenticazioni robuste, autorizzazioni granulari, controllo degli accessi, monitoraggio e segmentazione delle reti;
2. inventario e classificazione degli asset ICT, considerando esposizione su Internet, infrastrutture cloud e sistemi legacy non più supportati;
3. gestione delle vulnerabilità e delle patch, con individuazione e correzione più rapide, dando priorità ai sistemi esposti, al software open source e alle vulnerabilità zero-day;

4. monitoraggio, rilevazione e difesa, includendo il traffico da e verso i fornitori terzi e, quando proporzionato, strumenti di IA per identificare anomalie in tempo reale;
5. test di resilienza, risposta e recupero, mediante scenari realistici e progressivamente più complessi, comprensivi delle procedure di gestione delle crisi.

L'eventuale uso dell'intelligenza artificiale come strumento di difesa non è considerato una soluzione automaticamente affidabile. Deve essere coerente con la strategia aziendale sull'IA, preceduto da una valutazione dei rischi specifici e accompagnato da monitoraggio delle prestazioni e del loro eventuale deterioramento, nonché da un'adeguata supervisione umana.

La parte più operativa delle comunicazioni consiste nel coinvolgimento diretto degli organi societari.
Il consiglio di amministrazione, in una seduta congiunta con il collegio sindacale, dovrà esaminare la comunicazione e avviare la predisposizione di una relazione che, per ciascuna delle sei aree:

- rappresenti il livello attuale di esposizione al rischio;
- valuti l'adeguatezza dei presidi esistenti;
- individui carenze e priorità di intervento;
- definisca azioni, tempi e investimenti necessari;
-stabilisca come il consiglio di amministrazione verificherà l'avanzamento del piano.

L'impresa dovrà inoltre individuare e comunicare all'Autorità uno specifico punto di responsabilità aziendale, quale, ad esempio, la funzione di controllo dei rischi ICT di secondo livello. La relazione e il relativo piano di lavoro dovranno essere trasmessi a Banca d'Italia o a IVASS entro il 31 dicembre 2026.

Le entità interessate dovrebbero avviare immediatamente una gap analysis rispetto alle sei aree indicate, coinvolgendo consiglio di amministrazione, collegio sindacale, funzioni ICT, cybersecurity, risk management, compliance, internal audit e responsabili della gestione dei fornitori.

Occorre inoltre verificare che i contratti con cloud provider e altri fornitori ICT prevedano obblighi effettivi di cooperazione, monitoraggio della sicurezza, gestione tempestiva delle vulnerabilità, applicazione delle patch, continuità operativa e accesso alle informazioni necessarie.

CYBERSICUREZZA

27 Luglio 2026 – Commissione UE: pubblicata una guida operativa per le imprese sul Cyber Resilience Act.

La Commissione europea ha pubblicato il 27 luglio 2026 nuovi orientamenti sull'applicazione del Cyber Resilience Act – CRA, il Regolamento (UE) 2024/2847 che introduce requisiti obbligatori di cibersicurezza per prodotti hardware e software con elementi digitali. La guida, non vincolante, è rivolta in particolare a microimprese e PMI e chiarisce alcuni profili centrali del Regolamento: ambito di applicazione, software open source, modifiche sostanziali dei prodotti, periodi di supporto, valutazione dei rischi di cibersicurezza e obblighi di segnalazione.

Particolare attenzione è dedicata alla gestione della sicurezza lungo l'intero ciclo di vita del prodotto. I fabbricanti dovranno integrare i principi di security by design e by default, documentare i rischi considerati, gestire le vulnerabilità e assicurare aggiornamenti di sicurezza per un periodo adeguato alla vita utile prevedibile del prodotto.

La scadenza più vicina è l'11 settembre 2026. Da tale data i fabbricanti dovranno notificare a ENISA le vulnerabilità attivamente sfruttate e gli incidenti gravi che incidono sulla sicurezza dei prodotti. La prima segnalazione dovrà essere trasmessa entro 24 ore dalla conoscenza dell'evento, seguita dagli ulteriori aggiornamenti previsti dal Regolamento.

La maggior parte degli obblighi del CRA sarà invece applicabile dall'11 dicembre 2027.

Produttori, sviluppatori, importatori e distributori dovrebbero:

1. censire i prodotti hardware e software immessi sul mercato europeo;
2. verificare il proprio ruolo e gli obblighi applicabili nella catena di fornitura;
3. predisporre valutazioni documentate dei rischi di cibersicurezza;
4. definire periodi di supporto e procedure di gestione degli aggiornamenti;
5. organizzare entro l'11 settembre 2026 i flussi interni di rilevazione e notifica di vulnerabilità e incidenti;
6. aggiornare i contratti con fornitori e sviluppatori, disciplinando cooperazione, accesso alle informazioni e gestione delle vulnerabilità;
7. verificare se modifiche, integrazioni o personalizzazioni possano comportare una nuova valutazione di conformità;
8. coordinare gli obblighi CRA con NIS2, GDPR, DORA e normativa settoriale.

La pubblicazione della guida rappresenta un passaggio operativo importante: il CRA non richiederà soltanto prodotti sicuri al momento dell'immissione sul mercato, ma processi continuativi, documentati e verificabili di gestione del rischio cyber.

---

24 Luglio 2026 – Agenzia nazionale per la cybersicurezza: aggiornate le FAQ sulle misure di sicurezza per la supply chain dei soggetti NIS.

L'Agenzia per la Cybersicurezza Nazionale ha pubblicato nuovi chiarimenti interpretativi sul processo e i requisiti di sicurezza da implementare per proteggere la sicurezza della catena di approvvigionamento dei soggetti NIS 2, con l'obiettivo di agevolarne l'applicazione da parte dei soggetti interessati

Per supportare i soggetti NIS nell'adozione delle misure di sicurezza a protezione della loro supply chain, la FAQ MSB.13 indica le quattro fasi del relativo processo (valutazione del rischio associato alla fornitura; identificazione dei requisiti di sicurezza; enforcement dei requisiti e loro verifica).

Ai fini della valutazione del rischio associato alla fornitura, la FAQ MSB.14 ne elenca i criteri minimi da tenere in considerazione, mentre, con riferimento all'identificazione dei requisiti di sicurezza e al loro enforcement, le FAQ MSB.15 e MSB.16, rispettivamente, chiariscono che non è richiesto che tali requisiti siano definiti dal soggetto NIS per tutte le sue forniture e, conseguentemente, che non tutti i requisiti previsti dalle misure di sicurezza di base devono necessariamente essere ribaltati sul fornitore.

La FAQ MSB.17 specifica altresì che l'applicazione delle categorie di misure indicate dall'articolo 24 del decreto NIS, deve essere modulata fino alla eventuale esclusione di talune di esse (in funzione del contesto operativo, del livello di rischio e della criticità dei servizi affidati dalla singola Amministrazione) e la FAQ MSB.18 evidenzia che nei casi in cui l'operatore economico aggiudicatario sia costituito in forma di RTI, le misure di sicurezza possono essere soddisfatte dai soli componenti che erogano (anche parzialmente) la prestazione contrattuale che ha impatti sulla sicurezza informatica.

Infine, la FAQ MSB.19 precisa che, anche con riferimento ai contratti misti, l'applicazione dei requisiti di sicurezza deve essere modulata tenendo conto della loro proporzionalità, pertinenza e adeguatezza rispetto alle specifiche prestazioni affidate.

MERCATI DIGITALI

28 Luglio 2026 – La Francia è il primo Paese dell'UE a vietare i social network ai minori di 15 anni.

La Francia si prepara a diventare il primo Stato dell'Unione europea a vietare per legge l'accesso ai *social network* ai minori di quindici anni. L'entrata in vigore della legge è prevista per il 1° settembre 2026. La data non può tuttavia considerarsi ancora definitiva: il Conseil constitutionnel è stato investito del controllo di costituzionalità da due distinti ricorsi presentati da gruppi di oltre sessanta deputati. La promulgazione e l'effettiva applicazione della riforma dipenderanno quindi dall'esito di tale procedimento.

Il nuovo articolo 6-9 della legge francese sulla fiducia nell'economia digitale stabilisce che l'accesso ai servizi di social networking forniti da piattaforme online è vietato ai minori di quindici anni.
Per gli account creati prima del 1° settembre 2026, il divieto dovrebbe diventare operativo dopo un periodo transitorio di quattro mesi e, dunque, dal 1° gennaio 2027.

Sono escluse dal divieto:

- le enciclopedie online;
- i repertori educativi o scientifici;
- le piattaforme per lo sviluppo e la condivisione di software libero;
- i progetti digitali educativi open source.

La formulazione approvata non individua una specifica tecnologia obbligatoria per verificare l'età. Le piattaforme dovranno quindi adottare soluzioni di *age assurance* effettive, affidabili e coerenti con il quadro europeo, evitando che la verifica si riduca alla semplice dichiarazione della data di nascita da parte dell'utente.

La concreta applicazione del divieto dovrà essere coordinata con il Digital Services Act, con gli orientamenti della Commissione europea sulla protezione dei minori e con la disciplina sulla protezione dei dati personali.
Gli orientamenti europei raccomandano sistemi di verifica dell'età accurati, affidabili, robusti, non intrusivi e non discriminatori. La Commissione ha inoltre sviluppato un modello europeo che consente all'utente di dimostrare in modo anonimo il superamento di una determinata soglia di età, senza comunicare alla piattaforma l'identità, la data di nascita o ulteriori informazioni personali.
La riforma interviene anche sull'impiego degli smartphone negli istituti scolastici, estendendo alle scuole superiori il regime di limitazione già previsto per scuole elementari e medie.

La riforma francese mostra che la tutela dei minori sta diventando un requisito strutturale della progettazione dei servizi digitali. Per le piattaforme non sarà sufficiente modificare le condizioni generali: occorrerà dimostrare l'effettività dei controlli, la proporzionalità delle tecnologie adottate e la conformità dei sistemi di verifica dell'età alla disciplina europea sulla protezione dei dati.

---

22 Luglio 2026 – Corte di Giustizia UE: Google può essere ritenuta responsabile per i video YouTube di un creatore di contenuti vincolato da una partnership commerciale.

Il 19 luglio 2022 l'Autorità italiana per le Garanzie nelle Comunicazioni (AGCOM) ha irrogato a Google Ireland Ltd una sanzione di EUR 750 000 e le ha ordinato di rimuovere da YouTube diversi video che promuovevano i giochi d'azzardo online, in violazione della normativa italiana. Tali video erano stati pubblicati online da un creatore di contenuti vincolato a Google tramite un accordo di partnership commerciale che prevede, in particolare, una ripartizione dei ricavi provenienti dalla pubblicità trasmessa prima di ogni video. Tale accordo era stato preceduto da un controllo vertente sul contenuto dei video, sul tema del canale, sui video più visti o più recenti, nonché sui relativi metadati.

Google ha impugnato tale provvedimento dinanzi a un tribunale amministrativo italiano, invocando il diritto dell'Unione applicabile al commercio elettronico, e più in particolare il regime di deroga alla responsabilità di cui beneficiano gli hosting provider nei confronti dei contenuti pubblicati online da terzi. L'AGCOM ha sostenuto che tale regime non fosse applicabile nel caso di specie, poiché i giochi d'azzardo sono esclusi dall'ambito di applicazione della normativa europea relativa al commercio elettronico. Adito della controversia, il Consiglio di Stato italiano ha deciso di interpellare la Corte di giustizia.

Nella sua sentenza, la Corte rammenta anzitutto che il diritto dell'Unione esclude i giochi d'azzardo dall'ambito di armonizzazione in materia di commercio elettronico, nonché tutte le attività che vi sono connesse, a causa di considerevoli divergenze di ordine morale, religioso e culturale che sussistono in merito tra gli Stati membri. Tuttavia, l'attività di hosting online non è intrinsecamente connessa ai giochi d'azzardo, poiché essa consiste nella memorizzazione di contenuti forniti dall'utente in modo neutro, senza nessuna finalità di promozione. Di conseguenza, l'hosting di contenuti pubblicitari relativi ai giochi

d'azzardo online non rientra nell'esclusione prevista dal diritto dell'Unione, bensì invece nella normativa europea sul commercio elettronico. Inoltre, al fine di beneficiare della deroga alla responsabilità relativa ai contenuti pubblicati su una piattaforma, l'operatore deve agire in qualità di «prestatore intermediario», ossia svolgere un'attività puramente tecnica, automatica e passiva, che escluda qualsiasi conoscenza o controllo delle informazioni trasmesse o memorizzate. Ciò non si verifica qualora un operatore esamini, allo scopo di concludere un accordo di partnership commerciale, il tema principale di un canale di video, i video più visti o più recenti di tale canale, nonché i relativi metadati. L'operatore acquisisce pertanto una conoscenza concreta del contenuto essenziale di un insieme di video e non può quindi sostenere di agire in qualità di prestatore intermediario.

Spetta al giudice nazionale verificare, nell'ambito dell'accordo di partnership commerciale concluso con Google, se quest'ultima potesse ragionevolmente ignorare che il canale YouTube in questione aveva come tema principale i giochi d'azzardo e di fortuna e che quest'ultimo conteneva video che promuovevano siffatti giochi.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

25 Luglio 2026 – Organizzazione Mondiale della Proprietà Intellettuale: nel 2025 superata per la prima volta la barriera dei 10.000 miliardi di dollari in investimenti per beni immateriali.

Gli investimenti mondiali in attività immateriali hanno superato per la prima volta i 10.000 miliardi di dollari nel 2025, confermando il progressivo spostamento del valore economico dagli asset fisici verso software, dati, ricerca e sviluppo, marchi, design, competenze e capitale organizzativo.

È quanto emerge dalla terza edizione del World Intangible Investment Highlights 2026, pubblicata dall'Organizzazione mondiale della proprietà intellettuale – WIPO e dalla Luiss Business School. Il rapporto analizza 29 economie ad alto e medio reddito, rappresentative di circa il 57% del PIL mondiale.

Tra il 2008 e il 2025 gli investimenti immateriali sono cresciuti, in termini reali, a un ritmo 3,6 volte superiore rispetto a quelli in macchinari, attrezzature ed edifici. Nel solo periodo 2020-2025, nonostante l'aumento dei tassi di interesse e l'incertezza economica, la crescita media annua è stata del 5,5%, contro il 3,2% degli investimenti materiali. Gli intangibili rappresentano ormai il 12,8% del PIL delle economie analizzate, superando complessivamente la quota degli investimenti fisici.

La nozione economica di attività immateriale è più ampia rispetto a quella strettamente giuridica di proprietà intellettuale. Comprende infatti:

- ricerca e sviluppo;
- software e banche dati;
- marchi, reputazione e capacità di marketing;
- design;
- know-how e capitale organizzativo;
- processi, modelli operativi e reti commerciali;
- formazione e competenze del personale.

Una parte significativa di questi asset può essere protetta mediante brevetti, diritto d'autore, marchi, disegni e modelli, diritti sulle banche dati o disciplina dei segreti commerciali. Altri elementi, come procedure, competenze e capitale organizzativo, richiedono invece soprattutto adeguate misure contrattuali, organizzative e di riservatezza.

Il rapporto evidenzia inoltre che circa il 62% degli investimenti immateriali non viene rilevato dalle statistiche ufficiali. Il capitale organizzativo rappresenta oltre il 30% del totale, seguito dalla ricerca e sviluppo, con circa il 21%, dal software e dalle banche dati, dai marchi e dal design.

Software e banche dati costituiscono la categoria cresciuta più rapidamente, con un incremento medio annuo del 7,3% tra il 2013 e il 2023. Seguono il capitale organizzativo e i marchi, rispettivamente con tassi medi del 4,9% e del 4,4%.

I soli investimenti nei marchi hanno ormai superato la soglia di 1.000 miliardi di dollari, a conferma del ruolo assunto dalla reputazione, dalla fiducia dei consumatori e dalla capacità di differenziare prodotti e servizi nei mercati digitali e globalizzati.

Gli Stati Uniti concentrano quasi la metà degli investimenti immateriali considerati dal rapporto, con circa 5.000 miliardi di dollari nel 2025. Seguono il Giappone e la Germania. L'Italia registra investimenti stimati in circa 317 miliardi di dollari, ma figura tra le economie nelle quali, nel periodo 2015-2025, la componente materiale è cresciuta più rapidamente di quella immateriale.

Secondo WIPO e Luiss Business School, l'intelligenza artificiale sta alimentando due distinti cicli di investimento.

Il primo riguarda le infrastrutture materiali necessarie al funzionamento dei modelli avanzati: data center, semiconduttori, reti e sistemi energetici. Questa fase è attualmente molto concentrata negli Stati Uniti e presso un numero limitato di grandi operatori tecnologici.

La seconda ondata, destinata a produrre effetti più diffusi e duraturi, riguarda invece gli investimenti in dati, software, ricerca, competenze, marchi e riorganizzazione dei processi aziendali. Il valore generato dall'IA non dipenderà quindi soltanto dalla disponibilità della tecnologia, ma dalla capacità delle imprese di costruire e governare gli asset immateriali necessari per integrarla nei propri modelli operativi.

La crescita degli intangibili rende necessario affiancare agli investimenti tecnologici una specifica strategia di protezione e valorizzazione giuridica. Le imprese dovrebbero:

- effettuare un inventario periodico di software, database, marchi, brevetti, design, contenuti, modelli, algoritmi, know-how e processi proprietari;
- verificare la titolarità degli asset sviluppati da dipendenti, amministratori, consulenti, università, start-up e fornitori esterni;
- disciplinare nei contratti la proprietà dei risultati, le licenze, i diritti sugli sviluppi successivi e l'utilizzo di componenti di terzi;
- individuare il know-how strategico e adottare misure idonee a qualificarlo e conservarlo come segreto commerciale;
- proteggere marchi, nomi a dominio, design e altri segni distintivi nei mercati rilevanti;
- documentare provenienza, diritti di utilizzo e condizioni di licenza di dati e contenuti impiegati nei sistemi di IA;
- verificare le licenze del software open source e le possibili conseguenze sulla distribuzione dei prodotti;
- inserire gli asset immateriali nelle attività di due diligence, valutazione aziendale e gestione dei rischi;
- predisporre procedure per prevenire l'appropriazione o la dispersione di informazioni riservate in occasione della cessazione di rapporti di lavoro o collaborazione;
- coordinare la strategia di proprietà intellettuale con cybersecurity, data governance e conformità all'AI Act.

Il rapporto WIPO conferma che il vantaggio competitivo delle imprese risiede sempre meno nella sola disponibilità di beni fisici e sempre più nella capacità di creare, proteggere e sfruttare conoscenze, dati, tecnologie, reputazione e organizzazione. Investire negli asset immateriali senza definirne titolarità, protezione e condizioni di utilizzo può tuttavia determinare perdita di valore, contenziosi e difficoltà nelle operazioni di investimento o acquisizione.