FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 14/2026

DATA PROTECTION

14 Luglio 2026 – Corte di Giustizia UE: la pubblicazione online del nome degli atleti professionisti che hanno violato le norme antidoping non viola il diritto dell'Unione.

---

12 Luglio 2026 – Corte di Giustizia UE: la semplice pubblicazione online, a pagamento, di sentenze penali di condanna non costituisce un trattamento di dati personali a scopi giornalistici.

---

11 Luglio 2026 – Corte di Giustizia UE: un reclamo amministrativo all'Autorità di protezione dei dati personali e un ricorso giurisdizionale per lo stesso oggetto possono procedere in parallelo.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali – EDPB: approvate le Linee Guida 2/2026 sull'anonimizzazione. L'EDPB introduce un nuovo test giuridico e tecnico.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali: con le Linee Guida 3/2026 su web scraping e IA generativa, l'EDPB chiarisce quando il trattamento è conforme al GDPR.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali: approvate definitivamente, dopo la consultazione pubblica, le Linee Guida 2/2025 sul rapporto tra tecnologia Blockchain e GDPR.

INTELLIGENZA ARTIFICIALE

15 Luglio 2026 – Commissione UE: promosso il Codice europeo sulla trasparenza, il principale strumento per adempiere, dal 2 agosto prossimo, all'articolo 50 dell'AI Act.

---

12 Luglio 2026: Commissione UE: presentato il nuovo Piano d'Azione su cybersicurezza e Intelligenza Artificiale avanzata.

INFORMATION TECHNOLOGY

15 Luglio 2026 – Corte Suprema di Cassazione: il gestore di un blog è responsabile dei contenuti diffamatori pubblicati da terzi non rimossi.

CYBERSICUREZZA

14 Luglio 2026 – Agenzia nazionale per la cybersicurezza: aggiornate le FAQ su ruoli e compiti degli organi di amministrazione dei soggetti NIS.

---

14 Luglio 2026 – Autorità di sorveglianza del settore finanziario (ESAs): rilevante il rischio cyber sistemico per il settore finanziario derivante da modelli IA cosiddetti di frontiera.

MERCATI DIGITALI

14 Luglio 2026 – Autorità per le Garanzie nelle Comunicazioni: pubblicata la relazione sull'attività svolta da AGCOM come Coordinatore Nazionale ai sensi della Legge sui Servizi Digitali (DSA) nel 2025.

---

12 Luglio 2026 – Corte di Giustizia UE: respinto il ricorso della Apple contro la sua qualifica di *gatekeeper* ai sensi della Legge sui Mercati Digitali (Regolamento UE 2022/1925 – DMA) per Apple Store e iOS.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

15 Luglio 2026 – Disegni e modelli UE, pienamente applicabile il nuovo quadro normativo europeo.

---

15 Luglio 2026 – Ufficio europeo per la Proprietà Intellettuale – EUIPO: nel primo semestre 2026 numeri da record per le nuove registrazioni di marchi. Prima applicazione del nuovo sistema europeo di protezione delle indicazioni geografiche per i prodotti artigianali e industriali.

DATA PROTECTION

14 Luglio 2026 – Corte di Giustizia UE: la pubblicazione online del nome degli atleti professionisti che hanno violato le norme antidoping non viola il diritto dell'Unione.

La Commissione giuridica antidoping austriaca (ÖADR) e la Commissione indipendente di arbitrato austriaca (USK) hanno squalificato quattro atleti dalle competizioni nazionali e internazionali per un periodo determinato o a vita, per violazione delle norme antidoping. In forza della normativa austriaca, dette squalifiche sono pubblicate sul sito Internet dell'Agenzia austriaca antidoping (NADA Austria).

La pubblicazione comprende il nome e il cognome dell'atleta interessato, la disciplina sportiva praticata, la violazione delle norme antidoping commessa, la sanzione inflitta nonché l'inizio e la fine di quest'ultima. L'ÖADR pubblica, a sua volta, sul proprio sito Internet, tali dati nonché il nome della sostanza vietata eventualmente in questione.

I quattro atleti contestano dinanzi al Tribunale amministrativo federale austriaco il fatto che i loro nomi e gli sport interessati siano pubblicati sui siti Internet di cui trattasi. Essi ritengono, in particolare, che le informazioni pubblicate rientrino nella nozione di «dati relativi alla salute», il cui trattamento è in linea di principio vietato, nonché di dati personali relativi alle condanne penali e ai reati, il cui trattamento può essere effettuato, in linea di principio, solo sotto il controllo dell'autorità pubblica. Inoltre, essi sostengono che il regime indiscriminato di pubblicazione previsto in Austria è incompatibile con il regolamento generale sulla protezione dei dati (RGPD).

Il Tribunale amministrativo federale ha interrogato la Corte di giustizia al riguardo. La Corte risponde anzitutto che le informazioni pubblicate non rientrano, in linea di principio, nella nozione di «dati relativi alla salute», salvo il caso in cui il nome o la categoria della sostanza o del metodo vietato oggetto di detta violazione sia menzionato nella pubblicazione e tale menzione, unitamente ad altre informazioni relative alla persona interessata, sia tale da rivelare, anche indirettamente, mediante un'operazione intellettuale di raffronto o deduzione, informazioni sullo stato di salute fisica o mentale passato, presente o futuro di tale persona.

La Corte risponde poi che i dati personali relativi alle violazioni previste da una normativa nazionale antidoping e alle sanzioni inflitte per siffatte violazioni non costituiscono dati personali relativi alle condanne penali e ai reati. Infatti, tali violazioni e sanzioni riguardano solo un gruppo particolare di persone, vale a dire gli atleti, alla stregua delle sanzioni disciplinari aventi lo scopo di garantire il rispetto, da parte dei membri di un gruppo, di norme di comportamento proprie di quest'ultimo.

Infine, la Corte risponde che il RGPD, in linea di principio, non osta a una pubblicazione su Internet del nome degli atleti professionisti che hanno violato le norme antidoping, della durata della squalifica loro irrogata e dei motivi di quest'ultima. La lotta contro il doping, il cui scopo è quello di preservare lo svolgimento leale, integro e obiettivo della competizione sportiva, di garantire pari opportunità tra gli atleti, di tutelare la loro salute nonché di far rispettare i valori etici nello sport, costituisce un obiettivo di interesse generale. La pubblicazione delle violazioni delle norme antidoping è idonea a contribuire al conseguimento di tale obiettivo, contribuendo alla dissuasione, alla prevenzione e all'efficacia delle sanzioni. Per di più, la pubblicazione al di fuori di una cerchia ristretta di persone non sembra eccedere quanto necessario per realizzare detto obiettivo e, in particolare, per informare le persone sulle quali la sanzione grava indirettamente, incidendo anche sui loro interessi, quali i datori di lavoro e gli sponsor, attuali o potenziali, dell'atleta professionista sanzionato. Tuttavia, l'ente incaricato della pubblicazione deve poter procedere, prima della pubblicazione, a un bilanciamento individuale degli interessi in gioco per garantire che detta pubblicazione sia effettuata in modo conforme al RGPD e, in particolare, al principio di proporzionalità. Inoltre, un atleta interessato deve poter presentare un reclamo preventivo alla competente autorità per la protezione dei dati qualora vi siano indizi concreti che la pubblicazione che lo riguarda è imminente o avverrà in un prossimo futuro.

12 Luglio 2026 – Corte di Giustizia UE: la semplice pubblicazione online, a pagamento, di sentenze penali di condanna non costituisce un trattamento di dati personali a scopi giornalistici.

Una società svedese gestisce, a pagamento, una banca dati che consente di ricercare persone che sono state imputate in procedimenti penali e di consultare le sentenze di condanna che le riguardano. Una persona, condannata nel 2011, ha chiesto la cancellazione dei propri dati personali da tale banca dati. La cancellazione è tuttavia avvenuta solo in un momento successivo, sulla base della politica interna di conservazione dei dati di detta società. La persona in questione ha quindi presentato, dinanzi ai giudici svedesi, una domanda di risarcimento danni ai sensi del regolamento generale sulla protezione dei dati (RGPD). A sua difesa, la società ha invocato la tutela costituzionale di cui gode tale banca dati in virtù della libertà di espressione. Ai sensi del diritto svedese, tale tutela esclude l'applicazione del RGPD e lascia all'interessato, per far valere i propri diritti, soltanto la possibilità di proporre un'azione per diffamazione, in sede penale o civile.

Nutrendo dubbi sulla compatibilità di tale normativa con il RGPD, il giudice svedese ha interpellato la Corte di giustizia. Nella sua sentenza, la Corte rileva che il RGPD stabilisce che il diritto degli Stati membri concilia la protezione dei dati personali con la libertà di espressione e di informazione, e ciò anche a scopi giornalistici o di espressione accademica, artistica o letteraria. Gli Stati membri possono prevedere esenzioni e deroghe a talune disposizioni del RGPD, qualora ciò sia necessario per consentire tale conciliazione. Tuttavia, gli Stati membri non possono escludere l'applicazione del RGPD per trattamenti di dati che perseguano scopi diversi da quelli sopra indicati. Essi non possono neppure privare l'interessato dei mezzi di ricorso garantiti dal RGPD, lasciandogli soltanto la possibilità di proporre un'azione penale o civile per diffamazione. Infatti, tale persona deve poter esercitare, per quanto riguarda il trattamento dei propri dati personali, i mezzi di ricorso che tale regolamento le conferisce direttamente.

Secondo la Corte, i dati personali sono trattati a «scopi giornalistici» qualora tale trattamento abbia l'obiettivo di informare il pubblico o di condividere opinioni o idee, il contenuto sia preparato secondo regole deontologiche o etiche e sia oggetto di un lavoro di redazione o di adattamento, o, quanto meno, si inserisca in una linea editoriale. I fatti presentati devono essere stati verificati.
La pubblicazione online, a pagamento, delle condanne penali non sembra, fatta salva la verifica da parte del giudice nazionale, soddisfare tali condizioni e, pertanto, poter essere considerata diretta a perseguire tale scopo giornalistico.

---

11 Luglio 2026 – Corte di Giustizia UE: un reclamo amministrativo all'Autorità di protezione dei dati personali e un ricorso giurisdizionale per lo stesso oggetto possono procedere in parallelo.

Con la sentenza nella causa C-414/24, *Datenschutzbehörde*, la Corte di giustizia dell'Unione europea ha chiarito che un'autorità di controllo non può respingere un reclamo ai sensi dell'art. 77 GDPR per il solo fatto che, sulla stessa vicenda, sia già pendente un giudizio civile promosso ai sensi dell'art. 79 GDPR.

Il caso riguardava una professionista che aveva chiesto la cancellazione dei propri dati da una piattaforma di valutazione dei medici. Dopo il diniego del gestore, l'interessata aveva dapprima adito il giudice civile e successivamente presentato reclamo all'autorità austriaca per la protezione dei dati. Quest'ultima aveva dichiarato il reclamo inammissibile proprio a causa della pendenza del procedimento giudiziario.

La Corte ha ritenuto tale soluzione incompatibile con il GDPR. Il reclamo all'autorità di controllo e il ricorso giurisdizionale costituiscono infatti rimedi autonomi e concorrenti, destinati a svolgere funzioni diverse: il primo attiva i poteri di indagine, correttivi e sanzionatori dell'autorità; il secondo assicura la tutela davanti al giudice, anche ai fini dell'inibitoria e del risarcimento del danno.

Il rischio di decisioni contrastanti non giustifica, da solo, il rigetto del reclamo. Una simile impostazione potrebbe lasciare l'interessato privo di tutela qualora il giudizio civile si concludesse senza una decisione di merito, ad esempio per ragioni processuali, mentre nel frattempo fosse scaduto il termine per proporre reclamo.

La pronuncia conferma quindi che gli Stati membri possono disciplinare le modalità di coordinamento tra i due rimedi, ma non possono limitarne l'effettività né compromettere il livello di protezione garantito dal GDPR e dall'art. 47 della Carta dei diritti fondamentali dell'Unione europea.

La pronuncia, pur collocandosi nel solco dei precedenti *Hatóság* del 12 gennaio 2023, causa C-132/21, e *Schufa Holding (Esdebitazione)* del 7 dicembre 2023, cause riunite C-26/22 e C-64/22, è destinata a riaprire il dibattito sul coordinamento tra il reclamo all'autorità di controllo e il ricorso giurisdizionale previsti dal GDPR. La decisione assume particolare rilievo anche per l'ordinamento italiano, poiché l'art. 140-bis del Codice Privacy prevede un regime di alternatività tra reclamo al Garante e ricorso giurisdizionale. Alla luce della sentenza, tale disciplina potrebbe richiedere una nuova valutazione di compatibilità con il diritto dell'Unione.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali – EDPB: approvate le Linee Guida 2/2026 sull'anonimizzazione. L'EDPB introduce un nuovo test giuridico e tecnico.

Il Comitato europeo per la protezione dei dati ha adottato le nuove Linee guida 02/2026 sull'anonimizzazione, destinate ad aggiornare e sostituire il quadro interpretativo elaborato nel 2014 dal Gruppo di lavoro Articolo 29. Il documento, nella versione 1.0 del 7 luglio 2026, è stato sottoposto a consultazione pubblica fino al 30 ottobre 2026.

L'intervento dell'EDPB è particolarmente rilevante perché affronta uno dei temi più complessi della disciplina europea dei dati: stabilire quando un'informazione possa essere realmente considerata anonima e, quindi, sottratta all'applicazione del GDPR.

L'anonimizzazione è infatti spesso utilizzata per rendere disponibili dati a fini statistici, scientifici, analitici o di sviluppo di sistemi di intelligenza artificiale. Tuttavia, qualificare impropriamente come anonimo un insieme di dati ancora riconducibile a persone fisiche espone il titolare al rischio di trattare dati personali senza rispettare le condizioni e gli obblighi previsti dal Regolamento.
Le nuove Linee guida cercano di ridurre questa incertezza attraverso un modello che combina analisi giuridica, valutazione del contesto e verifica tecnica delle possibilità di identificazione.

Il punto centrale è che l'anonimato non costituisce necessariamente una qualità assoluta del dato. La stessa informazione può essere personale per un soggetto che dispone di mezzi o dati aggiuntivi utili all'identificazione e anonima per un altro che non abbia ragionevolmente accesso a tali risorse. La valutazione deve quindi essere condotta dalla prospettiva di tutti i soggetti rilevanti, inclusi titolare, destinatari ed eventuali responsabili del trattamento.

Il cuore operativo delle Linee guida è costituito da tre criteri destinati a verificare l'efficacia dell'anonimizzazione:

1. *No Record Isolation;*
2. *No Linkage;*
3. *No Inference.*

Se il dataset supera tutti e tre i criteri, può essere considerato anonimo. Il mancato superamento di uno di essi non determina automaticamente la natura personale dei dati, ma impone un'ulteriore analisi sul rischio effettivo di identificazione.

Il primo criterio, *No Record Isolation*, è soddisfatto quando il dataset non contiene combinazioni uniche di attributi riferibili a un singolo individuo.
L'eliminazione dei nomi non è sufficiente quando una persona può essere isolata attraverso una combinazione di sesso, data di nascita, codice postale, patologia, professione o altre caratteristiche. Più elevati sono il numero degli attributi e il livello di dettaglio, maggiore è la probabilità che una registrazione risulti unica.

Il secondo criterio, *No Linkage*, richiede che una registrazione non possa essere collegata, con certezza o elevata probabilità, a dati riguardanti la stessa persona presenti in altre fonti.
L'EDPB sottolinea che il collegamento può avvenire anche in assenza di identificativi comuni. Tecniche avanzate consentono di associare dataset attraverso combinazioni di caratteristiche, correlazioni, modelli comportamentali o informazioni ponte. Anche l'aggiunta intenzionale di rumore o inesattezze non esclude necessariamente il collegamento, poiché gli attacchi di record linkage possono tollerare un certo grado di imprecisione.

Il terzo criterio, *No Inference,* costituisce uno degli aspetti più innovativi del documento. Esso è soddisfatto quando dai dati non può essere ricavata un'inferenza al tempo stesso specifica e significativa su una persona identificata o identificabile.
L'inferenza è specifica quando riguarda un singolo individuo. È significativa quando può incidere sui suoi diritti o interessi, dipende effettivamente dal dataset e non deriva soltanto da conoscenze generali o da statistiche riferite alla popolazione.
Il criterio consente di intercettare anche forme sofisticate di ricostruzione dell'informazione: desumere l'abitazione e il luogo di lavoro da una sequenza di localizzazioni, ricavare uno stipendio individuale da statistiche aggregate, accertare la partecipazione di una persona al dataset originario oppure interrogare un modello di intelligenza artificiale per ottenere informazioni relative a uno specifico soggetto.

Le Linee guida assumono particolare rilievo per modelli di intelligenza artificiale, dati sintetici, statistiche aggregate e attività di ricerca. L'EDPB evidenzia infatti che tecniche di collegamento, de-aggregazione, *membership inference* e interrogazione dei modelli possono consentire di ricostruire informazioni individuali anche da dati apparentemente anonimi.

L'anonimizzazione deve inoltre essere valutata nel tempo. Il progresso tecnologico, la disponibilità di nuove fonti o un incidente di sicurezza possono rendere nuovamente identificabili dati inizialmente considerati anonimi.

Il processo di anonimizzazione resta, fino al suo completamento, un trattamento di dati personali e deve quindi rispettare il GDPR, compresi base giuridica, trasparenza e accountability. Il titolare deve documentare le tecniche applicate, i soggetti considerati, i test effettuati e le ragioni per cui il rischio di re-identificazione è stato ritenuto insignificante.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali: con le Linee Guida 3/2026 su web scraping e IA generativa, l'EDPB chiarisce quando il trattamento è conforme al GDPR.

L'EDPB ha adottato nuove Linee guida dedicate al web scraping utilizzato per lo sviluppo e l'addestramento di sistemi di intelligenza artificiale generativa, con l'obiettivo di chiarire le principali implicazioni privacy di una pratica sempre più diffusa.

Il *web scraping* consiste nell'estrazione automatizzata, spesso su larga scala, di dati disponibili online. Questa attività può avvenire senza che gli interessati ne siano consapevoli e può comportare rischi significativi per i loro diritti, soprattutto quando i dati raccolti vengono successivamente conservati, organizzati, analizzati o utilizzati per l'addestramento di modelli di IA.

L'EDPB chiarisce anzitutto che il GDPR trova applicazione ogni volta che il web scraping comporta operazioni su dati personali, quali raccolta, registrazione, conservazione, organizzazione, consultazione o recupero delle informazioni. La circostanza che i dati siano pubblicamente accessibili non li sottrae quindi, di per sé, alla disciplina europea sulla protezione dei dati.

Particolare attenzione deve essere prestata ai principi di limitazione della finalità e di trasparenza. Il titolare deve definire con precisione perché i dati vengono raccolti e verificare che il loro successivo utilizzo per l'addestramento dell'IA sia compatibile con tale finalità. Quanto agli obblighi informativi, l'EDPB riconosce che, in alcuni casi, informare individualmente tutti gli interessati può risultare impossibile o richiedere uno sforzo sproporzionato. Tale esenzione, tuttavia, non opera automaticamente e deve essere valutata alla luce delle concrete caratteristiche del trattamento.

Le Linee guida richiamano inoltre il principio di esattezza. L'EDPB raccomanda di acquisire dati soltanto da fonti affidabili, di registrare il momento in cui le informazioni sono state raccolte e di verificarne la correttezza prima dell'utilizzo nei dataset di addestramento. Ciò è particolarmente importante perché dati inesatti, obsoleti o decontestualizzati possono incidere sulla qualità del modello e produrre risultati erronei o lesivi per gli interessati.

Un ulteriore profilo centrale riguarda il principio di minimizzazione. Il titolare dovrebbe limitare la raccolta ai dati realmente necessari, adottare filtri preventivi, escludere categorie non pertinenti, definire criteri selettivi di acquisizione e prevedere misure tecniche e organizzative volte a ridurre il volume di dati personali trattati.

Le Linee guida sviluppano anche il tema della base giuridica. Riprendendo le indicazioni già contenute nel parere dell'EDPB sui modelli di IA, il Comitato fornisce chiarimenti sull'utilizzo del legittimo interesse ai sensi dell'articolo 6, paragrafo 1, lettera f), GDPR. Il titolare deve individuare un interesse legittimo concreto, dimostrare che il trattamento è necessario per perseguirlo e svolgere un effettivo bilanciamento con i diritti e le libertà degli interessati. La mera utilità economica o tecnica del web scraping non è sufficiente a giustificare automaticamente il trattamento.
Particolarmente delicato è il trattamento delle categorie particolari di dati personali. L'EDPB ricorda che il loro trattamento è, in linea di principio, vietato. Quando il web scraping intercetta dati relativi, ad esempio, alla salute, alle opinioni politiche, alla religione, all'origine etnica o all'orientamento sessuale, il titolare deve disporre sia di una base giuridica ai sensi dell'articolo 6 GDPR sia di una specifica condizione di liceità prevista dall'articolo 9, paragrafo 2.

Il Comitato richiama la sentenza della Corte di giustizia nella causa GC e altri, C-136/17, che potrebbe assumere rilievo nei casi in cui la raccolta di dati particolari sia soltanto incidentale o residuale. Tale impostazione può essere presa in considerazione solo se il titolare opera entro il perimetro delle proprie responsabilità, competenze e capacità e adotta adeguate misure tecniche e organizzative per impedire o limitare la raccolta e la diffusione di tali dati.
L'EDPB precisa però che non esiste alcuna esenzione generale dall'articolo 9 GDPR. Ogni trattamento deve essere valutato singolarmente, considerando la natura dei dati raccolti, la probabilità che emergano categorie particolari, le misure adottate per evitarne l'acquisizione e l'effettiva possibilità di eliminarle o separarle dal dataset.

Le nuove indicazioni sono destinate ad avere un impatto rilevante per sviluppatori di modelli di IA, fornitori di dataset, piattaforme digitali e imprese che utilizzano dati raccolti online: il web scraping non è vietato in quanto tale, ma deve essere progettato in modo selettivo, trasparente e proporzionato, con una preventiva valutazione della base giuridica, della necessità dei dati e dei rischi per gli interessati.

Le Linee guida saranno sottoposte a consultazione pubblica fino al 30 ottobre 2026, consentendo agli operatori del settore di formulare osservazioni e proposte prima dell'adozione definitiva.

---

10 Luglio 2026 – Comitato europeo per la protezione dei dati personali: approvate definitivamente, dopo la consultazione pubblica, le Linee Guida 2/2025 sul rapporto tra tecnologia Blockchain e GDPR.

Dopo la consultazione pubblica, l'EDPB ha adottato la versione definitiva delle Linee guida 02/2025 sul trattamento dei dati personali mediante tecnologie blockchain. Il documento chiarisce come le diverse architetture — pubbliche o private, *permissioned* o *permissionless* — incidano sugli obblighi previsti dal GDPR.
Il principio di fondo è che la compatibilità della blockchain con il GDPR dipende dall'architettura adottata, dalla governance e dalle garanzie incorporate fin dalla progettazione, non dalle caratteristiche della tecnologia considerate in astratto. Né la blockchain costituisce un'eccezione alla disciplina privacy. Prima di utilizzarla, l'organizzazione deve dimostrarne la necessità e la proporzionalità, individuare correttamente titolari, contitolari e responsabili del trattamento e verificare se le finalità possano essere raggiunte con soluzioni meno invasive.

L'EDPB raccomanda, in linea generale, di evitare la registrazione diretta di dati personali *on-chain.* Anche *hash, wallet address,* chiavi pubbliche, identificativi di transazione e metadati possono infatti costituire dati personali quando consentono di distinguere o collegare una persona. Cifratura e *hashing* restano misure di sicurezza e non determinano automaticamente l'anonimizzazione.

Particolare attenzione deve essere riservata all'immutabilità della blockchain, che può entrare in conflitto con i diritti di rettifica, cancellazione e limitazione. Il sistema deve quindi essere progettato fin dall'origine per consentire l'effettiva rimozione o anonimizzazione dei dati, ad esempio mantenendo le informazioni personali off-chain e registrando sulla catena solo elementi strettamente necessari.

Le Linee guida richiamano inoltre l'esigenza di individuare una valida base giuridica, gestire i trasferimenti internazionali derivanti dalla presenza di nodi extra SEE e svolgere una DPIA quando il trattamento presenta rischi elevati.

La versione finale delle Linee Guida rafforza i riferimenti alle tecnologie di tutela della riservatezza, comprese le prove a conoscenza zero, ma ribadisce che nessuna soluzione tecnica garantisce da sola la conformità.

INTELLIGENZA ARTIFICIALE

15 Luglio 2026 – Commissione UE: promosso il Codice europeo sulla trasparenza, il principale strumento per adempiere, dal 2 agosto prossimo, all'articolo 50 dell'AI Act.

La Commissione europea e il Comitato europeo per l'intelligenza artificiale hanno valutato positivamente il Codice di buone pratiche sulla trasparenza dei contenuti generati dall'IA, ritenendolo uno strumento adeguato per facilitare l'applicazione degli obblighi previsti dall'articolo 50, paragrafi 2, 4 e 5, dell'AI Act.

Il Codice, pubblicato il 10 giugno 2026, è uno strumento volontario rivolto ai fornitori e ai deployer di sistemi di IA generativa. La sua adesione non sostituisce gli obblighi direttamente previsti dall'AI Act, ma offre ai firmatari un quadro operativo riconosciuto a livello europeo per dimostrare la conformità alle regole sulla marcatura, rilevazione ed etichettatura dei contenuti artificiali.

La disciplina diventerà applicabile dal 2 agosto 2026. Da tale data, i fornitori di sistemi che generano o manipolano testi, immagini, audio o video dovranno assicurare che gli output siano contrassegnati in un formato leggibile automaticamente e rilevabili come artificialmente prodotti o modificati, nei limiti di quanto tecnicamente possibile. Le soluzioni adottate dovranno essere efficaci, interoperabili, solide e affidabili.

Per i deployer, il Codice riguarda in particolare l'obbligo di rendere riconoscibili i deep fake e i testi generati o manipolati dall'IA e pubblicati allo scopo di informare il pubblico su questioni di interesse generale. Per questi ultimi, l'obbligo incontra l'eccezione prevista dall'AI Act quando il contenuto sia stato sottoposto a revisione umana o controllo editoriale e una persona fisica o giuridica assuma la responsabilità della pubblicazione.

Il Codice è articolato in due sezioni. La prima è destinata ai fornitori e disciplina le misure tecniche per la marcatura e l'individuazione dei contenuti generati o manipolati. La seconda riguarda i deployer e stabilisce modalità comuni per informare gli utenti della natura artificiale dei deep fake e di determinate pubblicazioni testuali.

Tra le misure operative figurano l'impiego di marcature leggibili dalle macchine, il ricorso a standard aperti, lo sviluppo di meccanismi interoperabili di rilevazione e l'adozione di modalità di disclosure chiaramente percepibili dagli utenti. L'Unione ha inoltre predisposto un sistema comune di icone che creatori, editori e altri deployer possono utilizzare per segnalare la presenza di contenuti generati o manipolati mediante IA. Le icone sono liberamente utilizzabili, ma il loro impiego non determina, da solo, la conformità all'articolo 50: il deployer resta responsabile della chiarezza, visibilità e adeguatezza dell'informazione fornita.

La valutazione positiva assume particolare rilievo sul piano applicativo. I soggetti che aderiranno al Codice e ne attueranno correttamente le misure potranno utilizzarlo per dimostrare la conformità agli obblighi dell'AI Act, beneficiando di maggiore certezza giuridica, uniformità applicativa nell'Unione e riduzione degli oneri amministrativi. Chi sceglierà modalità alternative dovrà invece dimostrarne autonomamente l'adeguatezza, che potrà essere valutata caso per caso dalle autorità nazionali di vigilanza del mercato.

Il Codice non esaurisce tuttavia il quadro regolatorio. Sarà integrato dagli orientamenti della Commissione sull'articolo 50, destinati a chiarire quali soggetti e contenuti rientrino negli obblighi, come debbano essere applicate le eccezioni e quali modalità di marcatura ed etichettatura risultino concretamente appropriate.

Per imprese, editori, piattaforme e sviluppatori, l'indicazione operativa è quindi quella di mappare sin d'ora i contenuti prodotti o modificati mediante sistemi di IA, distinguere gli obblighi dei fornitori da quelli dei deployer, verificare le tecniche di marcatura disponibili e definire procedure interne per l'apposizione di etichette, icone e informazioni agli utenti.

L'adesione al Codice resta facoltativa, ma rappresenta la principale via comune indicata dalle istituzioni europee per tradurre l'articolo 50 dell'AI Act in misure tecniche e organizzative concretamente verificabili.

---

12 Luglio 2026: Commissione UE: presentato il nuovo Piano d'Azione su cybersicurezza e Intelligenza Artificiale avanzata.

La Commissione europea ha presentato il nuovo Piano d'azione dell'Unione europea sulla cybersicurezza e l'intelligenza artificiale. L'iniziativa intende offrire una risposta coordinata ai rischi derivanti dai modelli di IA più avanzati e, nello stesso tempo, valorizzarne l'impiego per rafforzare la prevenzione e la gestione degli attacchi informatici.

La Commissione parte dalla constatazione che l'intelligenza artificiale sta trasformando profondamente il panorama delle minacce cyber. Gli stessi strumenti che consentono di individuare vulnerabilità, analizzare grandi quantità di dati e reagire più rapidamente agli incidenti possono essere utilizzati anche da soggetti ostili per automatizzare gli attacchi, aumentarne la velocità e moltiplicarne la portata.

Il Piano si articola intorno a tre obiettivi: promuovere un uso sicuro e responsabile dell'IA avanzata, rafforzare la resilienza cibernetica europea e sviluppare capacità tecnologiche autonome dell'Unione nel settore della cybersicurezza basata sull'IA.

Un primo ambito di intervento riguarda la valutazione dei modelli avanzati di IA. La Commissione lancerà un'apposita iniziativa per creare una capacità europea di valutazione, anche sotto il profilo della cybersicurezza, che dovrebbe divenire operativa nel 2027. Tale struttura dovrà sostenere le funzioni regolatorie dell'AI Office e rafforzare la possibilità di sottoporre i modelli a verifiche indipendenti delle loro capacità, vulnerabilità e misure di mitigazione prima dell'immissione sul mercato europeo.

Il Piano affronta anche il problema dell'accesso ai sistemi di IA più potenti. La Commissione ed ENISA elaboreranno un modello europeo per consentire a soggetti pubblici e privati qualificati di accedere in modo strutturato e sicuro alle capacità dei modelli avanzati per finalità di cybersicurezza. L'obiettivo è evitare che l'accesso a tali tecnologie avvenga senza condizioni trasparenti o adeguate garanzie.

Un'altra misura centrale è la creazione, da parte di ENISA e del Centro comune di ricerca della Commissione, di una piattaforma protetta per testare soluzioni di IA applicate alla cybersicurezza, anche mediante ambienti simulati. Lo strumento sarà rivolto in particolare agli operatori di settori critici, tra cui finanza, energia, sanità, trasporti e pubblica amministrazione, affinché possano sperimentare e introdurre sistemi di IA senza esporre infrastrutture e dati reali a rischi non controllati.

Sul piano della resilienza, la Commissione invita le organizzazioni a rafforzare le pratiche di igiene informatica, la gestione del rischio e la sicurezza fin dalla progettazione. Le imprese e le amministrazioni dovrebbero inoltre utilizzare le capacità di IA già disponibili, compresi ove appropriato i modelli open source, per individuare e correggere più rapidamente le vulnerabilità e migliorare la prevenzione, il rilevamento e la risposta agli attacchi.

ENISA dovrà favorire la collaborazione tra autorità pubbliche, imprese e comunità open source, predisponendo orientamenti, raccomandazioni e buone pratiche. È prevista anche una specifica campagna per aumentare la sicurezza del software open source critico, componente ormai essenziale di numerosi sistemi e infrastrutture digitali.

INFORMATION TECHNOLOGY

15 Luglio 2026 – Corte Suprema di Cassazione: il gestore di un blog è responsabile dei contenuti diffamatori pubblicati da terzi non rimossi.

Il blogger che venga a conoscenza della presenza, sul proprio sito, di commenti diffamatori pubblicati da terzi è tenuto ad attivarsi tempestivamente per rimuoverli. L'inerzia successiva alla conoscenza dei contenuti illeciti può infatti determinare una responsabilità risarcitoria.

Il principio è stato ribadito dalla Corte di Cassazione con l'ordinanza 10 luglio 2026, n. 22999, relativa a una controversia originata da alcuni commenti denigratori pubblicati in calce a un post che contestava l'attendibilità di un articolo giornalistico.

Nel caso esaminato, il gestore del blog aveva mantenuto online i commenti anche dopo averne acquisito consapevolezza, provvedendo alla loro eliminazione soltanto a seguito dell'avvio del giudizio. I giudici di merito lo avevano pertanto condannato al risarcimento del danno non patrimoniale subito dal giornalista, quantificato in 23.000 euro sulla base dei criteri elaborati dal Tribunale di Milano in materia di diffamazione.

La Cassazione ha confermato la decisione, precisando che sul blogger non grava un obbligo generale di controllo preventivo dei contributi inseriti dagli utenti. La responsabilità sorge, tuttavia, quando il gestore, dopo essere venuto a conoscenza del carattere diffamatorio dei contenuti, ometta di rimuoverli con tempestività, consentendone l'ulteriore diffusione.

Secondo la Corte, la permanenza consapevole del commento lesivo equivale, sotto il profilo della responsabilità, a una forma di adesione o comunque di compartecipazione alla sua diffusione. La libertà di espressione garantita dall'articolo 10 CEDU non esclude, pertanto, l'obbligo di intervenire ex post a tutela della reputazione altrui.

La pronuncia si inserisce in un orientamento ormai consolidato, sia civile sia penale, che distingue nettamente tra l'assenza di un dovere di sorveglianza preventiva e l'obbligo di rimozione successivo alla conoscenza effettiva dell'illecito.

CYBERSICUREZZA

14 Luglio 2026 – Agenzia nazionale per la cybersicurezza: aggiornate le FAQ su ruoli e compiti degli organi di amministrazione dei soggetti NIS.

L'Agenzia per la Cybersicurezza Nazionale ha aggiornato le FAQ relative agli obblighi degli organi di amministrazione e direttivi dei soggetti NIS. L'aggiornamento fornisce indicazioni interpretative su alcuni aspetti applicativi della disciplina NIS 2, contribuendo a chiarire il ruolo degli organi di amministrazione e direttivi nell'ambito del sistema di governance della cybersicurezza.

Con riferimento alle responsabilità degli organi di amministrazione, si conferma che l'approvazione dei documenti previsti dall'articolo 23 del decreto NIS costituisce una competenza esclusiva dell'organo collegiale o, ove previsto, dell'organo monocratico e non può essere delegata. Rimane invece delegabile lo svolgimento delle attività necessarie all'attuazione operativa degli obblighi previsti dalla normativa.

Si precisa poi che i documenti da sottoporre all'approvazione degli organi di amministrazione devono definire gli indirizzi e la pianificazione strategica delle misure di sicurezza. La documentazione di natura

tecnica e operativa, quali procedure, istruzioni operative e manuali, può essere predisposta e aggiornata dalle strutture competenti senza necessità di approvazione da parte degli organi di governo.

Si chiarisce inoltre che i soggetti NIS possono organizzare la documentazione secondo le modalità ritenute più idonee, sia mediante un unico documento sia attraverso un insieme di documenti tra loro coordinati. L'aggiornamento dei documenti tecnici e organizzativi richiamati nella documentazione strategica non comporta la necessità di una nuova approvazione di quest'ultima.

---

14 Luglio 2026 – Autorità di sorveglianza del settore finanziario (ESAs): rilevante il rischio cyber sistemico per il settore finanziario derivante da modelli IA cosiddetti di frontiera.

L'EBA (European Banking Authority) l'EIOPA (European Insurance and Occupational Pensions Authority) e l'ESMA (European Securities and Markets Authority) hanno sostenuto l'avvertimento del Comitato europeo per il rischio sistemico (ESRB) sui rischi sistemici che i modelli di intelligenza artificiale di frontiera possono generare per il sistema finanziario europeo.

Secondo le autorità, questi modelli sono in grado di individuare e sfruttare vulnerabilità informatiche con maggiore rapidità, automatizzando attività offensive che in passato richiedevano tempi più lunghi e competenze specialistiche. Ne deriva un aumento della velocità, della scala e della sofisticazione degli attacchi, con particolare esposizione per banche, assicurazioni e intermediari.

Il rischio può assumere natura sistemica quando più operatori dipendono dagli stessi fornitori ICT, servizi cloud, modelli di IA o componenti software. La compromissione di un'infrastruttura condivisa potrebbe infatti propagarsi rapidamente tra numerose entità finanziarie e incidere sulla continuità dei servizi essenziali.
Le Autorità europee di vigilanza del settore bancario, finanziario e assicurativo invitano pertanto le imprese finanziarie ad aggiornare i propri framework di cybersicurezza, rafforzare la gestione delle vulnerabilità, ridurre i tempi di applicazione delle patch e predisporre test basati su scenari nei quali gli attaccanti utilizzano sistemi di IA avanzati. Tali rischi dovranno essere integrati nei presidi di resilienza operativa già richiesti dal regolamento DORA, compresi il controllo dei fornitori terzi, la gestione degli incidenti e i test di resilienza digitale.

Anche le autorità di vigilanza sono chiamate a includere l'evoluzione dell'IA nelle attività di supervisione, valutando sia l'utilizzo diretto dei modelli da parte delle imprese sia le minacce derivanti dal loro impiego da parte di soggetti ostili.

EBA, EIOPA ed ESMA continueranno a monitorare lo sviluppo dei modelli di frontiera, collaborando con le autorità nazionali e con i fornitori ICT. Il messaggio è chiaro: l'IA può rafforzare le capacità difensive, ma nel breve periodo può anche amplificare il rischio cyber e trasformarlo in una minaccia per la stabilità dell'intero sistema finanziario.

MERCATI DIGITALI

14 Luglio 2026 – Autorità per le Garanzie nelle Comunicazioni: pubblicata la relazione sull'attività svolta da AGCOM come Coordinatore Nazionale ai sensi della Legge sui Servizi Digitali (DSA) nel 2025.

AGCOM ha pubblicato la propria relazione annuale ai sensi dell'articolo 55 del Digital Services Act, relativa alle attività svolte dal 1° gennaio al 31 dicembre 2025 in qualità di Coordinatore dei servizi digitali per l'Italia.

Nel corso dell'anno, l'Autorità ha consolidato il proprio ruolo nell'attuazione del DSA, rafforzando la cooperazione con le altre autorità nazionali, con la Commissione europea e con il Comitato europeo per i servizi digitali.

Uno dei principali ambiti di attività ha riguardato la gestione dei reclami degli utenti ai sensi dell'articolo 53 DSA. Nel 2025 AGCOM ha adottato uno specifico regolamento procedurale e ha ricevuto circa 160 reclami, soprattutto relativi a misure ritenute sproporzionate rispetto ai diritti degli utenti, mancata o insufficiente motivazione di sospensioni o limitazioni degli account e difficoltà di accesso ai sistemi interni di reclamo delle piattaforme. Poiché tutti i casi riguardavano prestatori stabiliti fuori dall'Italia, AGCOM li ha trasmessi ai Coordinatori competenti dopo una valutazione preliminare.

Quanto agli ordini relativi a contenuti illegali e informazioni sugli utenti, nel 2025 non sono stati notificati ad AGCOM provvedimenti adottati da autorità nazionali ai sensi degli articoli 9 e 10 DSA. L'Autorità ha però adottato direttamente due ordini ex articolo 9 e quattro ordini ex articolo 10, condividendoli attraverso il sistema europeo AGORA.
Particolare rilievo ha assunto anche il riconoscimento dei *trusted flagger*, cioè dei cosiddetti segnalatori attendibili, quei soggetti qualificati che facilitano l'individuazione dei contenuti illegali e rendono più rapido ed efficace il meccanismo di *notice and action* previsto dal DSA. AGCOM ha ricevuto sedici domande e ne ha accolte dieci, respingendo le restanti sei per carenza dei requisiti previsti. È stata inoltre aggiornata la certificazione di ADR Center S.r.l. quale organismo di risoluzione extragiudiziale delle controversie, con ampliamento dei requisiti linguistici.

Sul fronte dell'accesso ai dati delle piattaforme da parte dei ricercatori accreditati, AGCOM ha collaborato con gli altri Coordinatori e con la Commissione per definire procedure armonizzate ai sensi dell'articolo 40 DSA e del regolamento di esecuzione UE 2025/2050. L'Autorità ha inoltre predisposto una pagina informativa e un helpdesk dedicato, anche se nel 2025 non sono state presentate richieste di accesso da parte di ricercatori italiani.
Per il 2026, AGCOM prevede di completare la mappatura dei prestatori soggetti al DSA, rafforzare la cooperazione con le autorità nazionali competenti sui contenuti illegali, valutare la creazione di una task force dedicata all'e-commerce e intensificare il dialogo con società civile e segnalatori attendibili.
Una priorità specifica sarà la tutela dei minori. L'Autorità intende sviluppare ulteriormente il quadro nazionale di attuazione dell'articolo 28 DSA e completare il lavoro sull'applicazione italiana di verifica dell'età collegata all'IT Wallet, nell'ambito delle iniziative europee dedicate a strumenti più efficaci di verifica dell'età.

La relazione mostra quindi un'attività ancora prevalentemente di coordinamento, gestione dei reclami e costruzione del quadro applicativo, ma anche un progressivo passaggio verso strumenti più strutturati di enforcement, cooperazione e protezione degli utenti vulnerabili.

---

12 Luglio 2026 – Corte di Giustizia UE: respinto il ricorso della Apple contro la sua qualifica di *gatekeeper* ai sensi della Legge sui Mercati Digitali (Regolamento UE 2022/1925 – DMA) per Apple Store e iOS.

Con le sentenze nelle cause riunite T-1079/23, T-1080/23 e T-214/24, la Corte di Giustizia della UE ha respinto i ricorsi proposti da Apple contro la decisione della Commissione che l'aveva designata come *gatekeeper* ai sensi del Digital Markets Act per l'App Store e il sistema operativo iOS. I ricorsi relativi a iMessage sono stati invece dichiarati irricevibili.

La Commissione aveva designato Apple il 5 settembre 2023 come *gatekeeper* per App Store, iOS e Safari. Nella stessa data aveva qualificato iMessage come servizio di comunicazione interpersonale indipendente dal numero e come servizio di piattaforma di base, avviando però un'indagine per verificare se ricorressero effettivamente le condizioni per la designazione. L'indagine si era conclusa nel febbraio 2024 senza includere iMessage tra i servizi per i quali Apple è gatekeeper.

Il Tribunale ha innanzitutto confermato che le diverse versioni dell'App Store — destinate a iPhone, iPad, Apple Watch, Mac e Apple TV — possono essere considerate un unico servizio di piattaforma di base. Pur operando su dispositivi differenti, esse perseguono infatti la stessa finalità: mettere in contatto gli sviluppatori con gli utenti finali e consentire la distribuzione delle applicazioni. Le differenze tecniche tra i dispositivi non sono state quindi ritenute sufficienti a configurare servizi distinti.

È stata inoltre dichiarata irricevibile l'eccezione con cui Apple contestava la validità della disposizione del DMA relativa agli obblighi di interoperabilità imposti ai gatekeeper. Secondo la Corte, tale norma non costituisce la base giuridica della decisione di designazione e non presenta con essa un collegamento giuridico diretto tale da consentirne la contestazione nell'ambito del ricorso contro la qualifica di gatekeeper.
La decisione conferma che, nella valutazione dei servizi digitali, la Commissione e il giudice europeo possono privilegiare la funzione economica sostanziale rispetto alle differenze tecniche o ai dispositivi sui quali il servizio viene offerto.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

15 Luglio 2026 – Disegni e modelli UE, pienamente applicabile il nuovo quadro normativo europeo.

Dal 1° luglio 2026 è pienamente operativo il nuovo quadro normativo dell'Unione europea sulla protezione dei disegni e modelli. La riforma, la più ampia realizzata nel settore da oltre vent'anni, mira a rendere il sistema più moderno, accessibile e adeguato allo sviluppo dei prodotti digitali e delle nuove tecnologie.

Il nuovo assetto è fondato sul Regolamento (UE) 2026/715 sui disegni e modelli dell'Unione europea, che raccoglie in un testo codificato la disciplina applicabile, completato dai nuovi regolamenti delegato e di esecuzione relativi alle procedure dinanzi all'EUIPO. La riforma europea comprende inoltre la direttiva (UE) 2024/2823, che dovrà essere recepita dagli Stati membri entro il 9 dicembre 2027 per armonizzare ulteriormente i sistemi nazionali.

La definizione di disegno o modello è stata ampliata per includere espressamente animazioni, movimenti e transizioni. Anche il concetto di prodotto comprende ora elementi non incorporati in oggetti fisici, quali interfacce grafiche, prodotti digitali e configurazioni spaziali di elementi. La tutela viene così adattata a realtà come applicazioni, ambienti virtuali, icone animate e altre creazioni prive di una forma materiale tradizionale.

Cambiano anche le modalità di deposito e rappresentazione. Le domande di registrazione dei disegni e modelli UE devono essere presentate direttamente all'EUIPO e non più attraverso gli uffici nazionali della proprietà industriale. Il nuovo sistema consente inoltre forme di rappresentazione più adatte ai prodotti dinamici e digitali, superando un modello costruito prevalentemente su immagini statiche. Le procedure sono state semplificate anche per le domande multiple. Non è più necessario che tutti i disegni o modelli inseriti nella stessa domanda appartengano alla medesima classe della classifica-zione di Locarno, con una maggiore flessibilità per le imprese che intendono proteggere collezioni o portafogli articolati di prodotti.

La riforma rafforza inoltre la protezione contro le nuove forme di contraffazione. Il titolare può intervenire anche rispetto alla creazione, al download, alla copia e alla condivisione di file o software contenenti il disegno protetto, destinati a consentire la riproduzione di un prodotto tramite tecnologie come la stampa 3D. È stata introdotta anche una specifica eccezione per gli atti compiuti a fini di riferimento, critica, commento, parodia o insegnamento, purché compatibili con le corrette pratiche commerciali e non pregiudichino indebitamente il normale sfruttamento del disegno o modello.

Sul piano visivo, i titolari possono utilizzare il simbolo Ⓓ per segnalare che il prodotto è protetto come disegno o modello registrato dell'Unione europea. L'indicazione non costituisce una condizione per la tutela, ma può agevolare la conoscibilità del diritto da parte dei terzi.

---

15 Luglio 2026 – Ufficio europeo per la Proprietà Intellettuale – EUIPO: nel primo semestre 2026 numeri da record per le nuove registrazioni di marchi. Prima applicazione del nuovo sistema europeo di protezione delle indicazioni geografiche per i prodotti artigianali e industriali.

Nel primo semestre del 2026, le domande di registrazione di marchi e disegni o modelli presentate all'EUIPO hanno raggiunto il livello più elevato mai registrato per i primi sei mesi dell'anno. Tra gennaio e

giugno sono state depositate complessivamente 166.214 domande, con un incremento del 4,7% rispetto allo stesso periodo del 2025.

La crescita è stata trainata soprattutto dai marchi dell'Unione europea. Le relative domande sono state 104.263, in aumento dell'8,4% su base annua e superiori anche al precedente record semestrale registrato nel 2021. Il dato conferma la crescente propensione delle imprese a proteggere i propri segni distintivi attraverso un titolo unitario valido in tutti gli Stati membri.

È aumentato in particolare il peso dei depositanti europei: la quota delle domande provenienti dall'Unione è passata dal 57,4% del 2025 al 60,7% del 2026. Tra gli Stati membri, la Germania si colloca al primo posto per numero di depositi, seguita da Italia, Spagna e Francia. A livello mondiale, la Cina resta il principale Paese di origine delle domande, nonostante una diminuzione del 12,4% rispetto al primo semestre dell'anno precedente.

Più stabile il quadro relativo ai disegni e modelli dell'Unione europea. Nel semestre sono state presentate 61.951 domande, con una lieve flessione dell'1% rispetto allo stesso periodo del 2025. La sostanziale tenuta dei depositi accompagna l'entrata nella fase conclusiva della riforma europea del design, pienamente applicabile dal 1° luglio 2026, che amplia la tutela alle creazioni digitali, alle animazioni e alle rappresentazioni dinamiche.

I dati mostrano che, in una fase di forte trasformazione tecnologica e competitiva, marchi e design continuano a rappresentare strumenti centrali per proteggere investimenti, identità aziendale e capacità di differenziazione sul mercato europeo. Per le imprese, il record dei depositi evidenzia anche la necessità di rafforzare le attività di sorveglianza sui nuovi titoli, verificare tempestivamente eventuali conflitti e integrare la proprietà industriale nelle strategie di sviluppo e internazionalizzazione.

Il semestre ha segnato anche la prima applicazione del nuovo sistema europeo di protezione delle indicazioni geografiche per i prodotti artigianali e industriali, operativo dal 1° dicembre 2025. L'EUIPO ha ricevuto 81 domande: 42 dal Portogallo, 25 dalla Francia e 10 dalla Slovacchia.
Il nuovo titolo consente di proteggere, a livello unitario, i nomi di prodotti artigianali e industriali le cui qualità, reputazione o caratteristiche siano essenzialmente riconducibili all'origine geografica. La competenza dell'EUIPO si estende così, oltre che ai marchi e ai disegni o modelli UE, anche alla gestione delle indicazioni geografiche relative a questa categoria di prodotti.