

## Aggiornamento Data protection, AI, IT and IP

n. 10/2026

### DATA PROTECTION

12 Maggio 2026 – La CNIL aggiorna le regole privacy per la valutazione del merito creditizio: più trasparenza su scoring, dati utilizzabili e decisioni automatizzate.

---

6 Maggio 2026 – La relazione delle attività del Data Protection Officer: la CNIL pubblica linee guida e modello operativo.

---

6 Maggio 2026 – Garante privacy: l’Autorità chiede maggiori poteri di intervento contro i deepfake.

---

### INTELLIGENZA ARTIFICIALE

12 Maggio 2026 – La Commissione UE prepara le linee guida sull’articolo 50 dell’AI Act: obblighi di trasparenza per chatbot, deepfake e contenuti AI.

---

12 Maggio 2026 – ANAC: il Bando tipo n. 2/2026 introduce l’obbligo di dichiarare l’uso dell’AI nelle gare per servizi di architettura e ingegneria.

---

7 Maggio 2026 - AI Act: Consiglio e Parlamento UE raggiungono un accordo provvisorio sul pacchetto “Omnibus VII” per semplificare l’attuazione delle regole sull’intelligenza artificiale.

---

4 Maggio 2026 – L’Autorità per le Garanzie nelle Comunicazioni - AGCOM invia una segnalazione alla Commissione europea sui servizi AI di Google.

---

4 Maggio 2026 – AI generativa: l’Antitrust impone più trasparenza sul rischio di “allucinazioni”.

---

### MERCATI DIGITALI

12 Maggio 2026 – Corte di Giustizia UE: gli Stati membri possono prevedere che gli editori di giornali abbiano diritto a un’equa remunerazione quando concedono ai prestatori di servizi online l’autorizzazione a utilizzare le loro pubblicazioni.

---

8 Maggio 2026 – Commissione UE: adottata una raccomandazione sulla verifica dell’età online per l’adozione da parte degli Stati Membri di strumenti comuni, anonimi e rispettosi della privacy entro il 2026.

---



**4 Maggio 2026 – Autorità per le Garanzie nelle Comunicazioni - AGCOM: nuova lista dei servizi di interesse generale online. Più visibilità per TV e radio su smart TV e interfacce digitali.**

---

**4 Maggio 2026 – Cina: il licenziamento motivato dalla sostituzione del lavoratore con l'AI non è automaticamente legittimo.**

---

### **INFORMATION TECHNOLOGY**

**4 Maggio 2026 – Pubblicità occulta sui social: il Consiglio di Stato sanziona i post che simulano esperienze personali di consumo.**

---

### **CYBERSICUREZZA**

**8 Maggio 2026 – Crisi e sicurezza nazionale: il DPCM 22 aprile 2026 rafforza il ruolo del CISR nel coordinamento strategico del Governo.**

---

### **PROPRIETA' INTELLETTUALE E INDUSTRIALE**

**7 Maggio 2026 - Prodotti artigianali e industriali: in vigore il D.lgs. 51/2026 sulle indicazioni geografiche "Non Agri".**

---

**5 Maggio 2026 – Corte Suprema di Cassazione penale: maglie da calcio contraffatte, i loghi dei club restano protetti anche penalmente.**

---

## DATA PROTECTION

### **12 Maggio 2026 – La CNIL aggiorna le regole privacy per la valutazione del merito creditizio: più trasparenza su scoring, dati utilizzabili e decisioni automatizzate.**

La CNIL ha pubblicato una [nuova raccomandazione](#) sull'utilizzo dei dati personali nell'ambito della [valutazione della solvibilità](#) dei richiedenti credito. Il documento, adottato all'esito di una consultazione pubblica avviata nel maggio 2025, mira a fornire agli operatori finanziari un quadro aggiornato per conformarsi al GDPR e alla legge nazionale sulla protezione dei dati (Loi Informatique et Libertés nei trattamenti connessi all'octroi de crédit).

La raccomandazione si concentra, in particolare, sui trattamenti effettuati per verificare la capacità del richiedente di adempiere alle proprie obbligazioni e rimborsare il finanziamento. La CNIL richiama l'esigenza di limitare i dati trattati a quelli pertinenti e strettamente necessari, anche quando vengano presi in considerazione precedenti inadempimenti contrattuali o informazioni provenienti da fonti interne ed esterne.

Particolare attenzione è dedicata agli strumenti di *scoring*, spesso parzialmente o integralmente automatizzati e, in alcuni casi, basati su sistemi di intelligenza artificiale. Alla luce della giurisprudenza della Corte di giustizia dell'Unione europea, in particolare nelle cause C-634/21 e C-203/22, la CNIL sottolinea che lo scoring può integrare una decisione automatizzata quando assume un ruolo determinante nella concessione del credito, con conseguente necessità di garantire agli interessati informazioni comprensibili sul funzionamento del meccanismo decisionale.

La raccomandazione rafforza quindi gli obblighi di trasparenza, accountability e controllo umano, richiamando anche la necessità di valutare l'eventuale svolgimento di una DPIA, di definire correttamente le basi giuridiche del trattamento, di limitare i tempi di conservazione e di assicurare misure di sicurezza adeguate. La CNIL ha inoltre pubblicato una [checklist operativa](#) per agevolare gli operatori nella verifica della conformità dei propri processi di valutazione della solvibilità.

La pubblicazione assume rilievo anche oltre il mercato francese, fornendo indicazioni valedoli in tutta la UE alla luce del GDPR e poiché conferma la crescente attenzione delle autorità europee verso l'uso di algoritmi, scoring e sistemi automatizzati nei servizi finanziari, soprattutto quando tali strumenti incidono sull'accesso al credito e sui diritti degli interessati.

---

### **6 Maggio 2026 – La relazione delle attività del Data Protection Officer: la CNIL pubblica linee guida e modello operativo.**

La CNIL, Autorità francese per la protezione dei dati, ha pubblicato sul proprio sito istituzionale [una guida dedicata alla relazione periodica delle attività del Data Protection Officer](#), corredata da un modello operativo scaricabile. Il documento qualifica la relazione del DPO non come un adempimento obbligatorio, ma come una buona prassi raccomandata, funzionale al governo della *compliance* e alla rendicontazione delle attività svolte verso il più alto livello della direzione aziendale.

Secondo la CNIL, la relazione può avere periodicità trimestrale, semestrale o annuale, in funzione delle caratteristiche dell'organizzazione, e dovrebbe consentire di diagnosticare lo stato dei principali trattamenti e progetti rilevanti, valutare i rischi giuridici, finanziari e reputazionali, documentare le misure di conformità adottate o in corso e individuare gli ostacoli ancora presenti nel percorso di maturazione privacy dell'ente.

Particolarmente rilevante è il collegamento con il ruolo istituzionale del DPO: la CNIL ricorda che, ai sensi del GDPR, il Data Protection Officer riferisce al livello più elevato della direzione. In questa prospettiva, la relazione diventa uno strumento di accountability interna, utile a rappresentare attività, pareri, raccomandazioni, indicatori chiave, eventuali criticità e fabbisogni organizzativi, senza che la richiesta di predisporre report periodici sia di per sé lesiva dell'indipendenza del DPO.

La guida valorizza inoltre la funzione della relazione come strumento di comunicazione e sensibilizzazione interna, anche verso collaboratori e rappresentanze del personale, al fine di rendere visibili i progressi compiuti e le attività ancora da realizzare. La CNIL suggerisce un approccio pragmatico: redigere il documento progressivamente nel corso dell'anno, utilizzare uno stile chiaro e conciso, integrare ove possibile dati, indicatori e rappresentazioni grafiche, e adattare il modello alle dimensioni, alle risorse, alla natura delle attività e alla sensibilità dei trattamenti svolti dall'organizzazione.

L'iniziativa appare significativa anche per il contesto italiano, in cui la funzione del DPO è sempre più chiamata a dimostrare concretamente il proprio contributo alla governance dei dati, alla gestione del rischio e alla costruzione di una cultura aziendale della protezione dei dati personali. La relazione periodica, pur non essendo espressamente imposta dal GDPR, può quindi rappresentare uno strumento utile per rafforzare tracciabilità, continuità, indipendenza sostanziale e visibilità della funzione privacy all'interno dell'organizzazione.

---

## **6 Maggio 2026 – Garante privacy: l'Autorità chiede maggiori poteri di intervento contro i deepfake.**

Il Garante per la protezione dei dati personali ribadisce che l'utilizzo di servizi che consentono di generare e condividere contenuti a partire da immagini o voci reali, arrivando anche a "spogliare" persone senza il loro consenso, possono determinare, oltre a possibili fattispecie di reato, gravi violazioni dei diritti e delle libertà fondamentali delle persone coinvolte, con tutte le conseguenze, anche sanzionatorie, previste dalla normativa europea in materia di protezione dei dati personali.

Già a dicembre 2025 l'Autorità ha adottato un [provvedimento di avvertimento](#) nei confronti degli utilizzatori di servizi basati sull'intelligenza artificiale, come Grok, ChatGPT e Clothoff - quest'ultima piattaforma già destinataria di un [provvedimento](#) di blocco nell'ottobre 2025 - e altri servizi analoghi disponibili online. L'Autorità, come segnalato in più occasioni, ribadisce la necessità di poter intervenire per interdire il collegamento dall'Italia a tali piattaforme di servizi.

Un potere di questo tipo permetterebbe di bloccare con tempestività la "catena virale" delle condivisioni e la diffusione incontrollata di dati e materiali dannosi.

La rapidità dell'intervento è fondamentale quando sono in gioco diritti fondamentali, come la protezione dei dati personali: una violazione in questo ambito può provocare danni gravi e spesso irreversibili.

---

## **INTELLIGENZA ARTIFICIALE**

### **12 Maggio 2026 – La Commissione UE prepara le linee guida sull'articolo 50 dell'AI Act: obblighi di trasparenza per chatbot, deepfake e contenuti AI.**

Dal 2 agosto 2026 l'Unione europea potrebbe aprire una nuova fase nella regolazione dell'intelligenza artificiale, imponendo obblighi più stringenti di trasparenza per chatbot, assistenti vocali, contenuti sintetici, deepfake e sistemi di riconoscimento delle emozioni o categorizzazione biometrica. È quanto emerge dalla bozza di linee guida della Commissione europea sull'articolo 50 dell'AI Act, documento ancora non vincolante ma già indicativo dell'approccio che Bruxelles intende adottare.

Il principio di fondo è che gli utenti devono poter capire quando stanno interagendo con un sistema di AI o quando un contenuto è stato generato o manipolato artificialmente. Non basteranno più avvisi generici o informazioni relegate nei termini d'uso: la comunicazione dovrà essere chiara, accessibile e collocata nel momento in cui l'utente entra in contatto con il sistema.

Le nuove regole riguarderanno in particolare quattro aree: l'obbligo di segnalare l'interazione uomo-macchina nei sistemi conversazionali; la marcatura dei contenuti sintetici in formato leggibile dalle macchine; l'informativa alle persone esposte a sistemi di riconoscimento delle emozioni o classificazione biometrica; e la dichiarazione dell'origine artificiale di deepfake e contenuti testuali generati dall'AI destinati a informare il pubblico su temi di interesse generale.

Uno dei punti più delicati riguarda la distinzione tra “provider” e “*deployer*”. Il primo è il soggetto che sviluppa o commercializza il sistema di AI; il secondo è chi lo utilizza sotto la propria responsabilità. La distinzione è rilevante perché gli obblighi non ricadono sempre sullo stesso soggetto: chi mette sul mercato un chatbot dovrà progettare in modo conforme, mentre chi lo usa per interagire con clienti o cittadini dovrà garantire che l’informazione arrivi correttamente all’utente finale.

Particolarmente complessa sarà la gestione dei contenuti sintetici. La Commissione richiama strumenti come *watermark*, metadati, *fingerprinting* o soluzioni crittografiche di provenienza, pur riconoscendo che non esiste oggi una tecnica unica in grado di risolvere ogni scenario. Per aziende, piattaforme e sviluppatori questo comporterà investimenti tecnici e organizzativi, con impatti più sensibili per startup, operatori open source e imprese che integrano modelli di terzi.

Il tema investe anche media, marketing e comunicazione aziendale. I deepfake non saranno rilevanti solo in ambito politico o informativo, ma anche nella pubblicità, nei podcast con voci clonate, nelle campagne con volti simulati e nei contenuti audiovisivi realistici. Per i testi generati dall’AI destinati a informare il pubblico, la bozza prevede una possibile esenzione quando vi sia revisione umana, controllo editoriale e responsabilità editoriale chiaramente individuabile.

Il mancato rispetto degli obblighi di trasparenza potrà comportare sanzioni significative: fino a 15 milioni di euro o, per le imprese, fino al 3% del fatturato annuo mondiale, se superiore. In questo quadro, la trasparenza non si presenta più soltanto come un adempimento regolatorio, ma come un elemento competitivo: chi saprà documentare processi, responsabilità e provenienza dei contenuti potrà rafforzare la propria affidabilità verso utenti, clienti e autorità di vigilanza.

---

## **12 Maggio 2026 – ANAC: il Bando tipo n. 2/2026 introduce l’obbligo di dichiarare l’uso dell’AI nelle gare per servizi di architettura e ingegneria.**

Con il Bando tipo n. 2/2026, approvato in via definitiva da ANAC con delibera n. 153 del 15 aprile 2026, l’intelligenza artificiale entra formalmente nella documentazione standardizzata delle gare pubbliche. La novità riguarda le procedure aperte per l’affidamento dei servizi di architettura e ingegneria di importo pari o superiore alle soglie europee, da aggiudicare secondo il criterio dell’offerta economicamente più vantaggiosa.

Il nuovo schema impone agli operatori economici di dichiarare se abbiano utilizzato sistemi di AI nella predisposizione dell’offerta tecnica e se intendano impiegare anche nella fase esecutiva. L’obbligo si fonda sull’art. 13 della legge n. 132/2025, che ammette l’impiego dell’intelligenza artificiale nelle professioni intellettuali solo per attività strumentali e di supporto, fermo restando il principio della prevalenza del lavoro umano.

La clausola ANAC apre però diversi nodi applicativi. La definizione di “sistema di IA”, mutuata dall’AI Act e richiamata dalla legge italiana, è ampia e può comprendere strumenti molto eterogenei: dai modelli generativi ai software specialistici per calcoli, progettazione o modellazione BIM assistita. In assenza di una tassonomia operativa chiara, gli operatori saranno chiamati a valutare autonomamente cosa dichiarare, con il rischio di comportamenti non uniformi.

Un ulteriore profilo critico riguarda la verificabilità delle dichiarazioni. La stazione appaltante riceverà dichiarazioni rese, di regola, ai sensi del d.P.R. 445/2000, ma resta incerto se esistano strumenti tecnici affidabili per accertare ex post l’effettivo uso dell’AI nella produzione di elaborati progettuali, calcoli, modelli BIM o documentazione tecnica. Il rischio è che l’obbligo resti un adempimento prevalentemente autodichiarativo o diventi terreno di nuovo contenzioso nelle gare.

Resta fermo, in ogni caso, il principio della responsabilità professionale. L’uso di strumenti di intelligenza artificiale non alleggerisce né trasferisce la responsabilità del professionista che valida, sottoscrive e firma gli elaborati. L’AI viene quindi ricondotta al ruolo di supporto tecnico-operativo, senza possibilità di invocarla come esimente rispetto alla qualità, correttezza o attendibilità della prestazione professionale.

Il Bando tipo n. 2/2026 segna così un passaggio rilevante nella regolazione dell’AI negli appalti pubblici: non vieta l’utilizzo della tecnologia, ma lo sottopone a trasparenza, tracciabilità dichiarativa e responsabilizzazione dell’operatore economico. La vera prova sarà ora l’applicazione pratica da parte di stazioni appaltanti e professionisti, soprattutto sulla definizione del livello di dettaglio richiesto nelle dichiarazioni e sulle modalità di controllo.

## **7 Maggio 2026 - AI Act: Consiglio e Parlamento UE raggiungono un accordo provvisorio sul pacchetto “Omnibus VII” per semplificare l’attuazione delle regole sull’intelligenza artificiale.**

La Presidenza del Consiglio dell’Unione europea e i negoziatori del Parlamento europeo hanno raggiunto un accordo provvisorio su una proposta volta a razionalizzare e semplificare talune disposizioni in materia di intelligenza artificiale. L’intervento si inserisce nel pacchetto legislativo c.d. “Omnibus VII”, parte dell’agenda europea di semplificazione normativa, e mira ad agevolare l’attuazione del Regolamento UE sull’intelligenza artificiale, riducendo alcuni oneri amministrativi e chiarendo il coordinamento tra AI Act e normativa settoriale.

Secondo quanto comunicato dal Consiglio, l’accordo intende garantire maggiore certezza giuridica agli operatori economici e un’applicazione più armonizzata delle regole nell’Unione, preservando al contempo il livello di tutela rispetto ai rischi connessi all’impiego dei sistemi di IA. La proposta originaria della Commissione prevedeva, tra l’altro, un adeguamento del calendario applicativo delle regole sui sistemi di IA ad alto rischio, l’estensione di alcune esenzioni previste per le PMI anche alle small mid-caps, modifiche mirate agli obblighi di conformità, il rafforzamento dei poteri dell’AI Office e una riduzione della frammentazione nella governance.

Uno degli aspetti centrali dell’accordo riguarda il differimento dell’applicazione delle disposizioni relative ai sistemi di IA ad alto rischio. I co-legislatori hanno individuato due date fisse: il 2 dicembre 2027 per i sistemi di IA ad alto rischio stand-alone e il 2 agosto 2028 per i sistemi di IA ad alto rischio incorporati in prodotti. Tale scelta sostituisce l’impostazione, inizialmente prospettata dalla Commissione, che collegava l’entrata in applicazione delle regole alla disponibilità degli standard e degli strumenti necessari.

L’accordo provvisorio introduce inoltre una nuova pratica vietata nell’ambito dell’AI Act, relativa alla generazione mediante sistemi di IA di contenuti sessuali o intimi non consensuali, nonché di materiale pedopornografico o di abuso sessuale su minori. Si tratta di un’integrazione rilevante del catalogo delle pratiche vietate, che rafforza il presidio normativo rispetto a utilizzi dell’IA particolarmente lesivi della dignità, dell’integrità e dei diritti fondamentali delle persone, con specifica attenzione alla protezione dei minori.

Sul piano degli obblighi di compliance, viene ripristinato l’obbligo, per i fornitori, di registrare nella banca dati UE i sistemi di IA quando essi ritengano che tali sistemi possano beneficiare di un’esenzione dalla qualificazione come sistemi ad alto rischio. Viene altresì confermato il requisito della “stretta necessità” per il trattamento di categorie particolari di dati personali ai fini dell’individuazione e correzione dei bias, in coerenza con l’esigenza di mantenere elevato il presidio di proporzionalità e minimizzazione nel trattamento di dati sensibili.

L’accordo interviene anche sui termini relativi agli strumenti di sperimentazione e trasparenza. Il termine per l’istituzione, da parte delle autorità nazionali competenti, delle regulatory sandboxes in materia di IA viene posticipato al 2 agosto 2027. Parallelamente, viene ridotto da sei a tre mesi il periodo di grazia concesso ai fornitori per implementare soluzioni di trasparenza relative ai contenuti generati artificialmente, con nuova scadenza fissata al 2 dicembre 2026.

Quanto alla governance, il testo chiarisce le competenze dell’AI Office in relazione alla supervisione dei sistemi di IA basati su modelli di IA per finalità generali, quando il modello e il sistema siano sviluppati dallo stesso fornitore. Sono tuttavia individuate specifiche eccezioni nelle quali restano competenti le autorità nazionali, tra cui i settori dell’attività di contrasto, della gestione delle frontiere, delle autorità giudiziarie e delle istituzioni finanziarie.

Particolare rilievo assume, infine, il coordinamento tra AI Act e normativa settoriale applicabile a prodotti industriali e regolamentati, quali dispositivi medici, giocattoli, ascensori, macchine e unità da diporto. I co-legislatori hanno concordato un meccanismo che consente di limitare l’applicazione delle prescrizioni dell’AI Act nei casi in cui la legislazione settoriale contenga requisiti specifici in materia di IA sostanzialmente analoghi, mediante atti di esecuzione. Per il settore delle macchine, è prevista un’esenzione dalla diretta applicabilità dell’AI Act, accompagnata dal conferimento alla Commissione del potere di adottare atti delegati nell’ambito del regolamento macchine per integrare requisiti di salute e sicurezza relativi ai sistemi di IA qualificati come ad alto rischio.

La Commissione sarà inoltre tenuta a fornire orientamenti agli operatori economici che immettono o utilizzano sistemi di IA ad alto rischio soggetti alla normativa armonizzata settoriale, al fine di agevolare l'adempimento degli obblighi previsti dall'AI Act e, al contempo, minimizzare gli oneri di conformità. Tale previsione appare particolarmente rilevante per le imprese operanti in filiere industriali regolamentate, nelle quali la sovrapposizione tra discipline di prodotto, sicurezza e requisiti specifici per l'IA rischia di generare duplicazioni documentali, incertezze interpretative e costi di compliance.

L'accordo resta, allo stato, provvisorio: dovrà essere approvato formalmente dal Consiglio e dal Parlamento europeo, per poi essere sottoposto alla revisione giuridico-linguistica e alla successiva adozione formale dell'atto legislativo. Le imprese che sviluppano, integrano o utilizzano sistemi di IA, in particolare se potenzialmente qualificabili come ad alto rischio, dovranno quindi monitorare l'evoluzione del testo definitivo e verificare tempestivamente l'impatto delle nuove scadenze e delle modifiche proposte sui propri programmi di compliance, governance dei dati, documentazione tecnica, procedure di gestione del rischio e rapporti contrattuali lungo la catena del valore.

---

#### **4 Maggio 2026 – L'Autorità per le Garanzie nelle Comunicazioni - AGCOM invia una segnalazione alla Commissione europea sui servizi AI di Google.**

L'Autorità per le garanzie nelle comunicazioni, nella sua qualità di *Coordinatore per i servizi digitali per l'Italia*, ha deciso di trasmettere alla Commissione europea una richiesta di valutazione dei servizi offerti da Google Ireland mediante le interfacce aperte al pubblico AIO (*AI Overviews*) e AI Mode, alla luce degli articoli 27, 34 e 35 del Digital Service Act - DSA.

L'iniziativa ha preso avvio da una segnalazione all'Autorità da parte della Federazione Italiana Editori Giornali – FIEG, che asserisce alcuni effetti pregiudizievoli per utenti, consumatori e imprese italiane derivanti dall'introduzione del servizio "*AI Overviews*" in Italia.

In particolare, FIEG ha segnalato una significativa riduzione della visibilità e reperibilità dei contenuti editoriali che, da un lato, metterebbe a repentaglio la sostenibilità economica degli editori e degli autori, in particolare di quelli più piccoli e indipendenti e, dall'altro, inciderebbe sulla libertà di espressione e di informazione e sul pluralismo delle fonti. Segnala inoltre il rischio che le risposte prodotte dall'IA contengano errori, imprecisioni o persino informazioni inventate (le cd. "allucinazioni"), senza offrire all'utente la possibilità di verificarne facilmente le fonti.

A seguito dell'acquisizione di informazioni fornite da Google e delle audizioni di Google, FIEG e FISC (Federazione Italiana Settimanali Cattolici), l'Autorità ha ritenuto di sottoporre la questione alla Commissione europea, ai sensi dell'articolo 65 del DSA, affinché quest'ultima ne valuti la fondatezza, ai fini dell'eventuale avvio di una indagine per la possibile violazione di alcuni obblighi previsti dal DSA in capo alle piattaforme e ai motori di ricerca di dimensioni molto grandi (le cd. VLOP/VLOSE) in materia di mitigazione dei rischi sistemici, tra cui quelli legati alla libertà di informazione e al pluralismo dei media (articoli 34 e 35 DSA), e di trasparenza dei sistemi di raccomandazione (articolo 27 DSA).

Il Consiglio dell'Autorità ha inoltre deciso, anche alla luce delle sue competenze in materia di tutela del diritto d'autore e di determinazione dell'equo compenso per l'utilizzo online di contenuti editoriali, l'istituzione di un tavolo permanente di confronto tra Google, altre piattaforme che intendessero aderire ed editori, con l'obiettivo di sviluppare un dialogo sui temi del copyright, dell'Intelligenza Artificiale e della tutela del pluralismo.

---

#### **4 Maggio 2026 – AI generativa: l'Antitrust impone più trasparenza sul rischio di "allucinazioni".**

L'AGCM rafforza il presidio consumeristico sui servizi di intelligenza artificiale generativa. Con tre istruttorie nei confronti di DeepSeek, Mistral AI e NOVA AI, l'Autorità ha affrontato il tema delle cosiddette "allucinazioni", ossia la generazione di contenuti inesatti, fuorvianti o inventati da parte dei chatbot. I procedimenti si sono conclusi con l'accoglimento degli impegni proposti dalle società, senza accertamento di infrazione ai sensi dell'art. 27, comma 7, del Codice del consumo.

Gli impegni assunti puntano a rendere più chiari, accessibili e tempestivi gli avvisi rivolti agli utenti, sia nei siti internet sia nelle app, anche nelle fasi che precedono la registrazione o l'acquisto del servizio. In particolare, le società dovranno inserire *disclaimer* permanenti nelle interfacce di utilizzo, sotto le chat, in lingua italiana e con link informativi dedicati, per avvertire gli utenti della possibilità che le risposte generate dall'AI contengano errori o informazioni non affidabili.

L'Autorità ha inoltre richiesto un rafforzamento dell'informativa precontrattuale, con avvertenze esplicite sui limiti di affidabilità dei contenuti prodotti dai sistemi di AI e sulla necessità di verificarne l'esattezza. Nel caso DeepSeek, gli impegni includono anche un investimento tecnologico volto a mitigare il fenomeno, pur prendendo atto che, allo stato attuale della tecnologia, le allucinazioni non possono essere eliminate integralmente.

Specifico anche l'intervento su NOVA AI: il servizio dovrà chiarire meglio al consumatore la propria natura di interfaccia unica di accesso a diversi chatbot, senza presentarsi come un sistema autonomo di aggregazione o rielaborazione delle risposte.

Nei provvedimenti l'AGCM ha valorizzato il fatto che l'informazione sul rischio di risposte inesatte sia rilevante per una scelta consapevole dell'utente, anche quando il servizio non comporta il pagamento di un corrispettivo monetario.

La vicenda conferma l'estensione della vigilanza sulle pratiche commerciali scorrette anche ai servizi di AI generativa.

---

## MERCATI DIGITALI

**12 Maggio 2026 – Corte di Giustizia UE: gli Stati membri possono prevedere che gli editori di giornali abbiano diritto a un'equa remunerazione quando concedono ai prestatori di servizi online l'autorizzazione a utilizzare le loro pubblicazioni.**

La Corte di giustizia è stata adita nell'ambito di un ricorso proposto da Meta contro una decisione dell'Autorità italiana per le garanzie nelle comunicazioni (AGCOM). Secondo Meta, la normativa italiana che istituisce un regime volto a garantire un'equa remunerazione per l'utilizzo online delle pubblicazioni di carattere giornalistico viola il quadro europeo relativo ai diritti degli editori nel mercato unico digitale.

La Corte [dichiara che il diritto a un'equa remunerazione per gli editori è compatibile con il diritto dell'Unione](#), a condizione che tale remunerazione costituisca il corrispettivo economico dell'autorizzazione all'utilizzo online delle loro pubblicazioni. Gli editori devono, inoltre, poter rifiutare tale autorizzazione o concederla a titolo gratuito. Peraltro, non può essere richiesto alcun pagamento ai prestatori che non utilizzano tali pubblicazioni.

Gli obblighi imposti ai prestatori di avviare trattative con gli editori, senza limitare la visibilità dei contenuti durante tale periodo, e di fornire i dati necessari per il calcolo della remunerazione, pur limitando la libertà d'impresa, appaiono giustificati, in quanto contribuiscono agli obiettivi del diritto dell'Unione di garantire il buon funzionamento e l'equità del mercato per il diritto d'autore e di consentire agli editori di recuperare i propri investimenti. Secondo la Corte, siffatti obblighi, che rafforzano la tutela degli editori, consentono di instaurare un giusto equilibrio tra la libertà d'impresa, da un lato, e il diritto di proprietà intellettuale, nonché il diritto alla libertà e al pluralismo dei media, dall'altro.

---

**8 Maggio 2026 – Commissione UE: adottata una raccomandazione sulla verifica dell'età online per l'adozione da parte degli Stati Membri di strumenti comuni, anonimi e rispettosi della privacy entro il 2026.**

La Commissione europea ha adottato una raccomandazione per promuovere, in tutta l'Unione europea, l'accesso a strumenti di verifica dell'età basati su tecnologie anonime di prova dell'età, con l'obiettivo di garantire elevati standard di tutela della privacy e protezione dei dati personali.

La misura si inserisce nella strategia europea di protezione e responsabilizzazione dei minori online, insieme ad altri interventi come l'applicazione del Digital Services Act, il *Piano d'azione contro il cyberbullismo* e la strategia *Better Internet for Kids*.

La raccomandazione invita gli Stati membri ad adottare entro il 31 dicembre 2026 soluzioni robuste e rispettose della privacy per la verifica dell'età, utilizzando il modello tecnico europeo predisposto dalla Commissione, adattabile alle esigenze nazionali e integrabile con i portafogli europei di identità digitale. Agli Stati membri viene inoltre raccomandato di predisporre piani di attuazione, collaborare con i coordinatori dei servizi digitali, con gli altri Stati membri, con la Commissione, i ricercatori e la società civile, nonché assicurare la conformità agli standard di cybersicurezza attraverso verifiche indipendenti di soggetti terzi.

La Commissione istituirà anche uno schema europeo di verifica dell'età, definendo i requisiti per i fornitori di attestazioni di prova dell'età e per le soluzioni di *age verification*. Saranno inoltre predisposti elenchi di soluzioni conformi agli standard europei di privacy e sicurezza e di fornitori affidabili in grado di verificare l'età degli utenti tramite strumenti come identità elettroniche, passaporti o carte d'identità.

Il tema si collega anche alle linee guida sulla protezione dei minori adottate dalla Commissione nell'ambito del Digital Services Act, che raccomandano l'impiego di metodi di *age assurance* efficaci, accurati, affidabili, robusti, non invasivi e non discriminatori, in particolare per limitare l'accesso dei minori a contenuti per adulti, come pornografia e gioco d'azzardo, o a servizi soggetti a limiti minimi di età.

Secondo la Commissione, il 24% dei ragazzi tra i 14 e i 17 anni in sei Paesi UE dichiara di vedere contenuti pornografici almeno una volta a settimana, dato che rafforza l'esigenza di strumenti di verifica dell'età efficaci, anche a supporto delle azioni di enforcement del DSA.

Il modello europeo consente agli utenti di dimostrare di avere superato una determinata soglia di età, ad esempio 15, 18 o 65 anni, senza rivelare l'età esatta né l'identità. La soluzione conferma soltanto il superamento della soglia richiesta e non comunica ulteriori informazioni né al fornitore dell'attestazione né alla piattaforma online.

La Commissione sottolinea che il sistema è progettato per garantire l'anonimato dell'utente, prevenire il tracciamento e assicurare piena coerenza con il quadro europeo del portafoglio di identità digitale. Il Regolamento europeo sull'identità digitale prevede infatti che gli Stati membri offrano gratuitamente ai residenti almeno un portafoglio europeo di identità digitale entro la fine del 2026, utilizzabile anche per condividere prove dell'età in modo sicuro e controllato dall'utente.

---

#### **4 Maggio 2026 – Autorità per le Garanzie nelle Comunicazioni - AGCOM: nuova lista dei servizi di interesse generale online. Più visibilità per TV e radio su smart TV e interfacce digitali.**

AGCOM ha pubblicato la lista dei servizi audiovisivi e radiofonici di interesse generale distribuiti online, in attuazione della delibera n. 250/25/CONS sulla revisione delle linee guida in materia di *prominence*. L'intervento si inserisce nel quadro dell'art. 29 del Testo unico dei servizi di media audiovisivi, che mira a garantire adeguato rilievo ai servizi di media di interesse generale su dispositivi, piattaforme e interfacce attraverso cui gli utenti accedono ai contenuti audiovisivi e radiofonici.

La lista, pubblicata sul sito dell'Autorità, individua i servizi che dovranno beneficiare di specifiche misure di visibilità negli ambienti digitali. L'elenco è articolato in cinque sezioni: servizi forniti dalla concessionaria del servizio pubblico, servizi commerciali audiovisivi nazionali, servizi commerciali audiovisivi locali, servizi commerciali radiofonici nazionali e servizi commerciali radiofonici locali. L'ordine di inserimento ha funzione meramente elencativa e non incide sui criteri di collocazione previsti dalle linee guida.

La disciplina riguarda, in particolare, la reperibilità dei servizi di interesse generale sulle interfacce di smart TV, decoder, dongle, box set, autoradio, sistemi di infotainment installati nei veicoli, radio domestiche e radio portatili. Restano invece esclusi, tra gli altri, smartphone, tablet, personal computer, console di gioco, smart speaker e dispositivi non connettabili a Internet privi di home page di navigazione.

Sul piano operativo, le linee guida prevedono che i servizi di interesse generale siano resi immediatamente visibili nella home page o nel primo livello di accesso del dispositivo, mediante apposite icone, righe o punti di accesso. Per le interfacce dei dispositivi televisivi, dopo l'icona di accesso ai canali del digitale terrestre, dovranno essere collocate le applicazioni dei servizi audiovisivi generalisti nazionali, seguite dalle applicazioni aggregate "Tv locali", "Tv nazionali" e "Radio".

La pubblicazione della lista rappresenta quindi un passaggio rilevante per l'assetto competitivo e regolatorio dell'ecosistema digitale: da un lato rafforza la tutela del pluralismo informativo e della diversità culturale; dall'altro impone a produttori di dispositivi, gestori di interfacce e fornitori di servizi media di adeguare le modalità di presentazione dei contenuti, evitando che la visibilità dei servizi di interesse generale sia rimessa esclusivamente a logiche commerciali o algoritmiche.

Le linee guida precisano inoltre che, in corrispondenza di ciascun aggiornamento della lista, i soggetti destinatari delle misure dovranno aggiornare i servizi di interesse generale sui dispositivi e sulle interfacce utente entro 60 giorni dalla pubblicazione della lista aggiornata. La qualifica di servizio di interesse generale potrà essere revocata qualora il servizio non rispetti più i requisiti previsti per l'inserimento nel relativo paniere.

---

#### **4 Maggio 2026 – Cina: il licenziamento motivato dalla sostituzione del lavoratore con l'AI non è automaticamente legittimo.**

Il Tribunale intermedio del popolo di Hangzhou si è pronunciato su un caso destinato ad assumere particolare rilievo nel dibattito internazionale sul rapporto tra automazione, intelligenza artificiale e tutela del lavoro. Secondo quanto reso noto dalla stampa cinese, la mera scelta dell'impresa di sostituire attività umane con sistemi di AI non integra, di per sé, una valida ragione di licenziamento.

La vicenda riguardava un dipendente di una società tecnologica attiva nel settore dell'intelligenza artificiale, assunto come supervisore del controllo qualità. Il lavoratore era incaricato di verificare l'affidabilità degli output generati da modelli linguistici, anche sotto il profilo della liceità dei contenuti, della protezione dei dati personali e della correttezza complessiva dei risultati prodotti dai sistemi automatizzati.

A seguito dell'evoluzione delle tecnologie utilizzate internamente, la società aveva ritenuto che parte delle mansioni potesse essere svolta direttamente dai sistemi di AI. Al dipendente era stata quindi proposta una diversa collocazione aziendale, su un ruolo inferiore e con una rilevante riduzione della retribuzione. A fronte del rifiuto del lavoratore, l'impresa aveva proceduto al licenziamento, invocando una riorganizzazione aziendale connessa al progresso tecnologico.

Il giudice cinese ha escluso che tale situazione potesse essere qualificata come "*cambiamento sostanziale delle circostanze oggettive*", nozione prevista dalla disciplina locale sui contratti di lavoro per giustificare, in determinati casi, la risoluzione del rapporto. Tale concetto, secondo il Tribunale, riguarda ipotesi eccezionali e strutturali, come operazioni societarie, trasferimenti o eventi tali da rendere oggettivamente impossibile la prosecuzione del contratto, circostanze non dimostrate nel caso concreto.

La decisione valorizza anche il profilo della ragionevolezza delle soluzioni alternative offerte al dipendente. Una ricollocazione con mansioni inferiori e una riduzione salariale significativa non è stata ritenuta idonea a soddisfare l'obbligo datoriale di ricercare misure eque nell'ambito di una riorganizzazione tecnologica. Il principio che emerge è particolarmente significativo: l'adozione di strumenti di intelligenza artificiale può certamente rispondere a esigenze di efficienza e competitività, ma non consente all'impresa di trasferire unilateralmente sui lavoratori i costi della trasformazione digitale. L'automazione, dunque, non equivale automaticamente a una legittima causa di recesso.

La pronuncia si inserisce in un contesto in cui la Cina sta promuovendo una crescente integrazione dell'AI nei processi produttivi, ma al tempo stesso segnala la necessità di accompagnare l'innovazione con adeguate garanzie occupazionali. Per le imprese, il messaggio è chiaro: la transizione tecnologica deve essere gestita attraverso percorsi ragionevoli di riorganizzazione, riqualificazione e dialogo con i lavoratori, senza sacrificare in modo sproporzionato la posizione del personale coinvolto.

## INFORMATION TECHNOLOGY

### **4 Maggio 2026 – Pubblicità occulta sui social: il Consiglio di Stato sanziona i post che simulano esperienze personali di consumo.**

Il Consiglio di Stato, con la sentenza n. 2871/2026, ha chiarito che i post diffusi sui social network sotto forma di esperienze personali di consumo possono integrare pubblicità occulta quando, in realtà, riproducono indicazioni e contenuti forniti dall'impresa ai propri venditori.

La decisione riguarda messaggi pubblicati su Facebook e Instagram, apparentemente presentati come testimonianze spontanee di consumatori sui benefici derivanti dall'uso di determinati prodotti. Secondo i giudici, tuttavia, tali contenuti avevano natura promozionale, poiché inseriti in una strategia commerciale diretta a valorizzare il prodotto e a reclutare nuovi aderenti, senza rendere riconoscibile il ruolo professionale dei soggetti che li diffondevano.

La pronuncia ribadisce un principio centrale in materia di pratiche commerciali scorrette: il consumatore deve poter distinguere chiaramente tra comunicazione personale e messaggio pubblicitario. Quando l'intento commerciale viene dissimulato attraverso registri comunicativi informali, emotivi o apparentemente privati, la condotta può assumere carattere ingannevole ai sensi del Codice del consumo.

Per le imprese che utilizzano venditori, *ambassador* o reti social per promuovere prodotti, la sentenza conferma quindi la necessità di adottare regole chiare di trasparenza, evitando contenuti che simulino esperienze spontanee o neutrali quando perseguono finalità commerciali.

---

## CYBERSICUREZZA

### **8 Maggio 2026 – Crisi e sicurezza nazionale: il DPCM 22 aprile 2026 rafforza il ruolo del CISR nel coordinamento strategico del Governo.**

Con il DPCM 22 aprile 2026 è stato adottato il regolamento di attuazione dell'art. 7-*bis*, comma 5, del D.L. n. 174/2015, relativo alla gestione delle situazioni di crisi che coinvolgono profili di sicurezza nazionale. Il provvedimento disciplina il funzionamento del Comitato interministeriale per la sicurezza della Repubblica (CISR) nei casi di crisi sistemiche, comprese quelle legate a minacce ibride e scenari cyber, che richiedano l'esercizio dei poteri di direzione, indirizzo e coordinamento del Presidente del Consiglio dei ministri.

Il decreto non introduce un sistema generale di gestione di tutte le emergenze, ma individua il perimetro entro cui il CISR opera quando la crisi assume rilievo per la sicurezza nazionale, lasciando ferme le competenze delle amministrazioni e degli altri organismi già previsti dall'ordinamento per crisi o emergenze prive di tale connotazione.

Tra le principali funzioni attribuite al CISR rientrano la formulazione di proposte al Presidente del Consiglio sugli indirizzi generali per la gestione della crisi, la valutazione del quadro informativo e delle sue evoluzioni, l'individuazione di misure e provvedimenti da adottare anche ai fini dell'eventuale intervento del Consiglio dei ministri, nonché la promozione di esercitazioni per rafforzare la capacità sistemica di risposta.

Particolare rilievo assume la dimensione cibernetica: nelle crisi che coinvolgono aspetti di cybersicurezza, il CISR è integrato con la partecipazione del Ministro delegato per l'innovazione tecnologica e la transizione digitale e del direttore generale dell'Agenzia per la cybersicurezza nazionale. Il Presidente del Consiglio può inoltre modulare la composizione del Comitato in base alla natura della crisi, coinvolgendo ministri competenti, vertici della protezione civile, consiglieri diplomatici e militari, direttori di AISE e AISI, nonché altre autorità civili o militari.

Il decreto introduce anche la Strategia di sicurezza nazionale, da adottare su proposta del CISR, sentito il COPASIR, e da aggiornare almeno ogni tre anni. La Strategia dovrà individuare gli interessi fondamentali da tutelare, gli obiettivi strategici, le politiche e gli strumenti di prevenzione e contrasto dei fattori di minaccia e rischio, nonché gli indirizzi generali per la gestione unitaria delle crisi.

Un ruolo centrale è attribuito al CISR tecnico, chiamato a svolgere attività preparatorie, istruttorie, di analisi informativa, coordinamento e monitoraggio dell'attuazione delle misure. In caso di crisi particolarmente gravi e urgenti, il CISR tecnico potrà essere convocato con modalità semplificate e restare riunito in via permanente fino alla cessazione della crisi.

Nel complesso, il DPCM rafforza il coordinamento politico-strategico della Presidenza del Consiglio nelle crisi che incidono sugli interessi fondamentali della Repubblica, valorizzando il raccordo informativo tra istituzioni, la prevenzione organizzativa e l'integrazione della dimensione cyber e ibrida nella sicurezza nazionale.

---

## PROPRIETA' INTELLETTUALE E INDUSTRIALE

### **7 Maggio 2026 - Prodotti artigianali e industriali: in vigore il D.lgs. 51/2026 sulle indicazioni geografiche "Non Agri".**

È entrato in vigore il D.lgs. 2 aprile 2026, n. 51, che adegua l'ordinamento italiano al Regolamento (UE) 2023/2411 sulla protezione delle indicazioni geografiche per i prodotti artigianali e industriali, applicabile a livello europeo dal 1° dicembre 2025.

Il nuovo quadro normativo introduce un sistema uniforme di tutela per prodotti non agroalimentari caratterizzati da un forte legame con il territorio di origine, quali ceramiche, vetri, tessuti, gioielli, pizzi, porcellane, cuoi e manufatti in legno. La protezione potrà riguardare sia prodotti realizzati artigianalmente, anche con strumenti digitali, sia prodotti industriali o realizzati in serie, purché ricorrano i requisiti previsti dal regolamento: origine geografica determinata, qualità, reputazione o altra caratteristica essenzialmente attribuibile a tale origine e svolgimento di almeno una fase produttiva nella zona delimitata.

Il decreto individua nel Ministero delle imprese e del made in Italy, tramite l'UIBM, l'autorità competente per la fase nazionale della procedura di registrazione. La domanda dovrà essere presentata telematicamente e contenere il disciplinare di produzione, il documento unico e la documentazione di accompagnamento. La procedura prevede un esame nazionale, l'eventuale fase di opposizione e, in caso di esito positivo, la trasmissione della domanda all'EU IPO per la fase europea, destinata a concludersi con una registrazione efficace in tutta l'Unione.

Particolare rilievo assume la disciplina transitoria prevista per i nomi già protetti o acquisiti con l'uso storico. I soggetti interessati potranno avvalersi di una procedura semplificata per ottenere la registrazione europea come indicazione geografica protetta, così da preservare la continuità della tutela dei nomi già radicati sul mercato.

Il D.lgs. 51/2026 introduce inoltre un apparato di controlli e sanzioni volto a garantire l'effettività della protezione. Il MIMIT è competente per i controlli ufficiali e il monitoraggio dell'uso dei nomi registrati, anche online. Sul piano penale, viene modificato l'art. 517-quater c.p., estendendo la tutela contro la contraffazione delle indicazioni geografiche anche ai prodotti artigianali e industriali. Sul piano amministrativo, sono previste sanzioni pecuniarie graduate in base alla gravità della violazione, oltre all'inibizione all'uso dell'indicazione protetta e, nei casi più rilevanti, alla pubblicazione del provvedimento.

Il nuovo sistema rappresenta un passaggio significativo per la valorizzazione giuridica del patrimonio manifatturiero e artigianale italiano. Per associazioni di produttori e imprese sarà ora essenziale mappare i segni geografici in uso, verificare la sussistenza dei requisiti di protezione e valutare tempestivamente l'accesso alla procedura di registrazione, anche al fine di trasformare una reputazione territoriale consolidata in un diritto di proprietà intellettuale tutelato a livello europeo.

---

### **5 Maggio 2026 – Corte Suprema di Cassazione penale: maglie da calcio contraffatte, i loghi dei club restano protetti anche penalmente.**

Con la sentenza n. 10236/2026, la Suprema Corte di Cassazione ha confermato la rilevanza penale della vendita di magliette recanti loghi, stemmi o segni distintivi contraffatti di società calcistiche.

Il caso riguardava la condanna di un soggetto per commercio di prodotti con segni falsi e ricettazione, a seguito della detenzione per la vendita di capi che riproducevano elementi riconducibili a squadre di calcio. La difesa aveva sostenuto che non si trattasse di veri marchi, ma di semplici immagini, scritte o riferimenti a calciatori e club sportivi. La Suprema Corte ha respinto questa impostazione, ribadendo che le società



calcistiche professionistiche operano anche come imprese commerciali e possono registrare e valorizzare economicamente i propri segni distintivi. Loghi ed emblemi apposti sull'abbigliamento sportivo ufficiale non hanno quindi una funzione meramente decorativa, ma servono a identificare prodotti collegati alla notorietà e all'attività della squadra. Da qui la conferma dell'applicabilità dell'art. 474 c.p.: la detenzione per la vendita di magliette con marchi calcistici contraffatti integra il reato di commercio di prodotti con segni falsi.

La Corte ha inoltre ritenuto correttamente motivata anche la condanna per ricettazione, valorizzando, tra l'altro, la mancata indicazione di una provenienza lecita dei beni.

Esclusa, infine, la particolare tenuità del fatto. Secondo i giudici, il numero dei prodotti contraffatti e i precedenti specifici dell'imputato non consentivano di qualificare l'offesa come minima né il comportamento come occasionale.

La decisione conferma quindi un orientamento ormai consolidato: il merchandising sportivo ufficiale è pienamente tutelato anche sul piano penale, e la riproduzione non autorizzata dei segni dei club può esporre a responsabilità non secondo quanto previsto dal codice civile e dal Codice della Proprietà Industriale, ma anche in base alle norme dell'ordinamento penale.

---