Digital Omnibus

La semplificazione del corpus digitale europeo:

AI Act, GDPR, NIS2, DORA e Data Act a confronto

Nota al lettore

Questo documento ha finalità divulgative e informative. Ricostruisce, in forma sintetica ma ragionata, lo stato di un processo legislativo europeo ancora in evoluzione. La parte principale del dossier espone le modifiche annunciate, il loro contesto e le diverse posizioni emerse nel dibattito pubblico, senza assumere una posizione favorevole o contraria alla riforma.

La postfazione finale ha invece una natura diversa. Non introduce nuove informazioni normative e non sostituisce l'analisi giuridica: propone una lettura interpretativa sul rapporto tra tempi della regolazione e velocità dell'evoluzione tecnologica, in particolare nel campo della cybersicurezza e dell'intelligenza artificiale. È quindi una divagazione ragionata, collocata dopo il dossier proprio per distinguerla dal corpo informativo principale.

Le date, le soglie e gli stati dell'iter riportati riflettono la situazione a maggio 2026. Poiché il pacchetto non è ancora interamente adottato in via definitiva, alcuni elementi possono cambiare prima della pubblicazione nella Gazzetta Ufficiale dell'Unione europea.

Il documento non costituisce consulenza legale. Per decisioni operative occorre fare riferimento ai testi ufficiali e a un parere professionale qualificato.

1. Che cos'è il Digital Omnibus

Il Digital Omnibus è un'iniziativa legislativa annunciata dalla Commissione europea nel novembre 2025 e formalmente presentata, nei suoi atti principali, il 19 novembre 2025. Il suo obiettivo dichiarato è semplificare, consolidare e chiarire il cosiddetto corpus digitale dell'Unione: l'insieme di norme che, negli ultimi anni, hanno regolato dati, cybersicurezza e intelligenza artificiale.

La Commissione lo presenta come la prima fase di un più ampio percorso di razionalizzazione del quadro normativo digitale europeo. L'idea di fondo è ridurre duplicazioni, disallineamenti e incertezze applicative senza smantellare l'impianto regolatorio costruito negli anni precedenti.

Tecnicamente non si tratta di un'unica norma, ma di un pacchetto composto da due proposte di regolamento distinte:

• il Digital Omnibus, talvolta indicato come Digital Legislation Omnibus, che interviene tra l'altro su GDPR, Direttiva ePrivacy, Direttiva NIS2 e Data Act;

• il Digital Omnibus on AI, o AI Omnibus, che modifica alcuni profili del Regolamento sull'intelligenza artificiale, l'AI Act.

Il pacchetto si inserisce nel più ampio Digital Package, annunciato nello stesso giorno, che comprende anche una Data Union Strategy sull'uso dei dati nell'IA e l'iniziativa degli European Business Wallets. Nel linguaggio della Commissione, l'operazione è presentata come una misura di competitività e semplificazione: meno oneri amministrativi, maggiore certezza giuridica e regole più coerenti tra loro.

In sintesi

Il Digital Omnibus non crea nuove materie regolate. Interviene su norme già esistenti per ridurne le sovrapposizioni, chiarirne l'applicazione e allinearne alcune scadenze. Non è un testo unico del digitale europeo, ma una serie di modifiche mirate a più atti normativi.

2. Perché è nato: il problema delle sovrapposizioni

Negli ultimi anni l'Unione europea ha approvato in rapida successione un insieme di norme digitali: la Direttiva NIS2 sulla cybersicurezza, il Regolamento DORA sulla resilienza operativa digitale del settore finanziario, l'AI Act sull'intelligenza artificiale, il Cyber Resilience Act sui prodotti digitali, il Data Act sui dati generati dai dispositivi connessi, oltre al GDPR, già applicabile dal 2018.

Queste norme sono nate in momenti diversi e per finalità diverse. Il risultato è un panorama in cui la stessa organizzazione può ricadere contemporaneamente sotto più regimi, con autorità competenti, scadenze, moduli, obblighi di documentazione e procedure di notifica non sempre coordinati.

La Commissione riferisce che la proposta nasce da oltre un anno di lavoro preparatorio e da un'ampia consultazione. Imprese di settori diversi avevano segnalato problemi di sovrapposizione regolatoria, attuazione disomogenea tra Stati membri e difficoltà nel tradurre norme diverse in procedure aziendali coerenti.

Un esempio concreto è la notifica degli incidenti. Prima del pacchetto, un soggetto colpito da un incidente informatico poteva essere tenuto a segnalarlo separatamente sotto NIS2, DORA, GDPR e altri regimi, con tempistiche e canali differenti. Il Digital Omnibus cerca di ridurre proprio questo tipo di duplicazione.

3. Che cosa cambia, norma per norma

La tabella seguente riassume le principali aree di intervento. I dettagli sono sviluppati nei paragrafi successivi.

Norma interessata	**Principali interventi proposti**
AI Act	Rinvio delle scadenze per i sistemi ad alto rischio; chiarimenti sugli obblighi di conformità; semplificazione di alcune procedure di valutazione; nuovo divieto relativo a sistemi usati per generare materiale di abuso sessuale su minori o immagini intime non consensuali.
GDPR	Proposta di chiarimento/modifica della nozione di dato personale e del trattamento dei dati pseudonimizzati, con riferimento ai mezzi ragionevolmente utilizzabili per identificare una persona; soglia di notifica delle violazioni elevata al solo rischio elevato; termine esteso a 96 ore. Punto tra i più controversi del pacchetto.
ePrivacy	Integrazione delle regole sui cookie nel quadro del GDPR; rifiuto con un clic; divieto di richieste di consenso ripetute per la stessa finalità; segnali di preferenza leggibili da macchina.
NIS2 / DORA / CER	Proposta di punto unico di accesso, Single-Entry Point, per la notifica degli incidenti secondo il modello report once, share many; modelli e procedure armonizzati, ove adottati nel testo finale.
Data Act	Consolidamento nel quadro del Data Act di strumenti oggi separati, tra cui Data Governance Act, Regolamento

	sul libero flusso dei dati non personali e Open Data Directive; semplificazione di alcuni obblighi.

3.1 Le modifiche all'AI Act

L'intervento sull'AI Act è quello che ha avuto l'evoluzione più rapida. La ragione è soprattutto temporale: secondo il testo dell'AI Act in vigore, gli obblighi per i sistemi ad alto rischio avrebbero iniziato ad applicarsi il 2 agosto 2026. Commissione e co-legislatori si sono quindi mossi per intervenire prima di quella data.

Nelle prime ore del 7 maggio 2026, dopo una sessione di trilogo e un primo tentativo fallito il 28 aprile, Parlamento europeo e Consiglio hanno raggiunto un accordo politico provvisorio sul Digital Omnibus on AI. L'accordo deve ancora essere adottato formalmente da entrambe le istituzioni e sottoposto a revisione giuridico-linguistica. L'obiettivo dichiarato è completare l'adozione prima del 2 agosto 2026.

Le nuove scadenze per i sistemi ad alto rischio

L'elemento più rilevante dell'accordo è lo spostamento delle date di applicazione degli obblighi per i sistemi ad alto rischio. Il meccanismo condizionale inizialmente proposto dalla Commissione viene sostituito da date fisse:

• 2 dicembre 2027 per i sistemi ad alto rischio autonomi, elencati nell'Allegato III, ad esempio sistemi usati per reclutamento, riconoscimento delle emozioni o credit scoring;

• 2 agosto 2028 per i sistemi ad alto rischio integrati in prodotti già regolati da altre normative europee di sicurezza, cioè quelli dell'Allegato I.

La motivazione è pratica. L'infrastruttura di supporto alla conformità, composta da standard armonizzati, organismi notificati, documenti di orientamento e procedure di valutazione, non sarebbe stata pronta entro agosto 2026. Diverse analisi indicano che gli standard armonizzati non saranno disponibili nella loro completezza prima della fine del 2026 e che in vari Stati membri la designazione delle autorità nazionali competenti è in ritardo rispetto al calendario originario.

Un punto spesso frainteso

Il rinvio delle scadenze non equivale, di per sé, a un indebolimento delle regole. L'architettura dell'AI Act basata sul rischio resta in piedi e gli obblighi sostanziali per i

sistemi ad alto rischio non vengono cancellati. L'orologio viene spostato indietro, non spento. Le organizzazioni devono quindi usare il tempo aggiuntivo per prepararsi, non per rimandare il problema.

Il nuovo divieto sui contenuti abusivi

Parallelamente alla semplificazione, l'accordo introduce un nuovo divieto nell'ambito dell'articolo 5 dell'AI Act. Il divieto riguarda i sistemi di IA usati per generare materiale di abuso sessuale su minori o immagini intime non consensuali, comprese le cosiddette app di nudification.

Il divieto si applica in tre configurazioni: l'immissione sul mercato di sistemi finalizzati a generare tali contenuti; l'immissione sul mercato di sistemi privi di ragionevoli misure di sicurezza per prevenirne la generazione; l'uso da parte dei deployer per tale finalità. Le imprese avrebbero tempo fino al 2 dicembre 2026 per adeguare i sistemi interessati. Questo punto è stato indicato dai negoziatori del Parlamento come una priorità della loro posizione.

Etichettatura dei contenuti generati e altri aspetti

L'obbligo di marcatura dei contenuti sintetici, previsto dall'articolo 50(2) dell'AI Act per audio, immagini, video e testi generati artificialmente, viene fissato al 2 dicembre 2026. La data è più ravvicinata rispetto a quella inizialmente proposta dalla Commissione, che indicava il 2 febbraio 2027.

L'accordo affronta inoltre il rapporto tra AI Act e legislazione settoriale di sicurezza dei prodotti, il punto più conteso nel primo trilogo. La soluzione individuata è restrittiva: per i prodotti-macchina dotati di IA si applicano in via principale le regole settoriali, con salvaguardie dirette a garantire un livello equivalente di salute e sicurezza. Viene infine posticipato al 2 agosto 2027 il termine per l'istituzione, a livello nazionale, degli spazi di sperimentazione normativa, o sandbox.

3.2 Il punto unico di notifica degli incidenti

Sul versante della cybersicurezza, l'intervento più concreto proposto dal Digital Omnibus generale è la creazione di un Single-Entry Point, un punto unico di accesso per la segnalazione degli incidenti. Allo stato, si tratta di una proposta ancora soggetta al negoziato legislativo. L'idea è costruita sulla piattaforma di notifica già prevista dal

Cyber Resilience Act e affidata a ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, che dovrebbe sviluppare e gestire un portale sicuro a livello europeo.

Il principio operativo è riassunto nella formula report once, share many: segnalare una volta, condividere con molti. Se adottato, il meccanismo potrebbe consentire a un'organizzazione di assolvere, con un unico invio, obblighi di notifica previsti da più atti, tra cui NIS2, DORA, Direttiva CER, Regolamento eIDAS e GDPR. La portata effettiva dipenderà tuttavia dal testo finale, dai modelli armonizzati, dalle interfacce tecniche e dall'integrazione con le autorità competenti.

Questo non significa che gli obblighi sostanziali scompaiano. Il punto unico semplifica il canale di trasmissione, ma non elimina automaticamente le responsabilità previste dai diversi regimi né sostituisce le autorità competenti. La Commissione sarebbe inoltre incaricata di armonizzare contenuti e modelli delle segnalazioni, riducendo la frammentazione procedurale.

In parallelo, sul fronte GDPR, gli obblighi di notifica sovrapposti previsti dalla Direttiva ePrivacy per i fornitori di servizi di comunicazione verrebbero abrogati. La notifica delle violazioni sotto GDPR sarebbe richiesta solo quando la violazione presenta un rischio elevato per gli individui, con un termine esteso a 96 ore. Si tratta di un cambiamento rilevante rispetto allo standard attuale, che richiede la notifica salvo quando è improbabile che la violazione comporti un rischio.

3.3 Le modifiche su dati personali e cookie

Le proposte sul GDPR sono tra le più discusse del pacchetto. Il testo proposto interviene su punti sensibili: la definizione di dato personale, il trattamento di dati pseudonimizzati, la notifica delle violazioni e l'uso residuale di categorie particolari di dati personali durante lo sviluppo e il funzionamento di sistemi di IA.

La modifica più delicata riguarda l'identificabilità. La nozione di dato personale verrebbe collegata in modo più esplicito ai mezzi ragionevolmente utilizzabili per identificare una persona. Inoltre, la Commissione riceverebbe il potere di specificare, con il contributo del Comitato europeo per la protezione dei dati, criteri relativi ai dati pseudonimizzati e alla loro qualificazione in determinati contesti. È uno dei punti più controversi del pacchetto: le autorità europee di protezione dei dati hanno segnalato il rischio che modifiche apparentemente tecniche incidano in modo sostanziale sul perimetro delle garanzie del GDPR.

Il pacchetto introdurrebbe anche un'esenzione per il trattamento residuale di categorie particolari di dati personali durante lo sviluppo e il funzionamento di sistemi di IA, purché siano rispettate specifiche salvaguardie. È uno degli aspetti che richiede maggiore cautela interpretativa, perché incide su un equilibrio centrale del GDPR: consentire innovazione e addestramento dei sistemi senza svuotare le garanzie per gli interessati.

Sul fronte dei cookie, l'obiettivo dichiarato è ridurre la consent fatigue, cioè la stanchezza da consenso. Le regole chiave sull'accesso ai dispositivi verrebbero spostate nel quadro del GDPR. Sono previste un'opzione di rifiuto con un clic, il divieto di prompt di consenso ripetuti per la stessa finalità entro un certo periodo e le basi per segnali di preferenza automatizzati e leggibili da macchina, che i titolari dovrebbero rispettare una volta adottati gli standard.

4. A che punto è l'iter legislativo

È essenziale distinguere i due binari del pacchetto, perché procedono a velocità diverse.

Il Digital Omnibus on AI ha seguito un percorso accelerato. Presentato a novembre 2025, ha raggiunto un accordo politico provvisorio in trilogo il 7 maggio 2026. Restano da completare l'adozione formale da parte di Parlamento e Consiglio, la revisione giuridico-linguistica e la pubblicazione definitiva. L'obiettivo politico è arrivare prima del 2 agosto 2026.

Il Digital Omnibus generale, cioè quello che incide su GDPR, ePrivacy, NIS2 e Data Act, procede invece secondo la tempistica ordinaria. A maggio 2026 non ha ancora raggiunto un accordo politico. È entrato nella procedura legislativa ordinaria e sarà quindi esaminato, discusso ed emendato da Parlamento e Consiglio prima dell'adozione di un testo definitivo.

A questo si affianca un secondo momento del percorso di semplificazione: un più ampio digital fitness check, uno stress test dell'intero corpus digitale europeo. La consultazione pubblica collegata si è chiusa l'11 marzo 2026; l'adozione di questa seconda fase è prevista per il 2027.

Avvertenza sullo stato dei testi

Finché i testi definitivi non sono pubblicati, date, soglie e formulazioni restano provvisorie. Le proposte possono essere modificate nel negoziato politico e tecnico. Per questo le informazioni riportate sono una base di orientamento e pianificazione, non una garanzia sul contenuto finale della normativa.

5. Il dibattito: posizioni a confronto

Il pacchetto ha suscitato letture diverse. Riportarle separatamente aiuta a distinguere la logica dichiarata della riforma, le preoccupazioni istituzionali e le critiche provenienti dalla società civile.

5.1 La lettura della Commissione e dei sostenitori

Per la Commissione europea, il Digital Omnibus è uno strumento di competitività e snellimento normativo: un riordino, non una deregolamentazione. L'obiettivo è ridurre gli oneri amministrativi, in particolare per piccole e medie imprese, eliminare duplicazioni e aumentare la certezza giuridica senza intaccare i livelli di protezione.

In questa prospettiva, allineare le scadenze dell'AI Act alla disponibilità effettiva degli strumenti di conformità è una misura di realismo regolatorio: evita di imporre obblighi tecnici quando gli standard e le procedure necessarie non sono ancora pienamente disponibili.

5.2 Le preoccupazioni di una parte del legislatore

All'interno dello stesso Parlamento europeo non mancano posizioni caute. Alcuni gruppi hanno avvertito che il consolidamento normativo potrebbe produrre un quadro meno coerente, con strutture poco chiare per le autorità di vigilanza e regimi di conformità ancora frammentati.

Il timore è che semplificare la forma non semplifichi necessariamente la sostanza. Un testo più compatto può infatti restare difficile da applicare se gli obblighi continuano a sovrapporsi o se le autorità nazionali interpretano in modo diverso le nuove procedure.

5.3 Le critiche della società civile

Organizzazioni per i diritti digitali e per i diritti umani hanno espresso riserve più nette, soprattutto sulle modifiche al GDPR. Secondo questa lettura, ridefinire ciò che costituisce dato personale e ampliare le possibilità di trattamento per lo sviluppo di sistemi di IA rischierebbe di indebolire tutele che, finora, sono state considerate un riferimento globale per la privacy.

Viene inoltre criticata l'ambiguità di alcune formule, come l'obbligo di rimuovere dati dai sistemi di IA solo quando ciò non richieda sforzi sproporzionati. Espressioni di questo tipo possono diventare, secondo i critici, punti di incertezza applicativa e spazi di interpretazione troppo ampi.

5.4 Un punto di equilibrio

Una lettura intermedia considera l'AI Omnibus come un intervento a doppio movimento: semplificazione dove i costi di conformità erano elevati e irrigidimento dove i rischi sono ritenuti più acuti. Il rinvio delle scadenze per i sistemi ad alto rischio convive infatti con l'introduzione del nuovo divieto sui contenuti abusivi.

La direzione di marcia, quindi, non è univoca. Il pacchetto non può essere letto solo come deregolamentazione, ma nemmeno come semplice rafforzamento delle tutele. È piuttosto un tentativo di ricalibrare un impianto normativo cresciuto rapidamente e non sempre in modo coordinato.

6. Che cosa significa, in pratica

Per le organizzazioni che operano nel mercato unico, alcune implicazioni emergono già con ragionevole chiarezza, pur nella provvisorietà dei testi.

• Più tempo, non meno lavoro. Chi sviluppa o impiega sistemi di IA ad alto rischio dispone di un orizzonte più lungo, tra fine 2027 e metà 2028, ma gli obblighi sostanziali restano e la preparazione è attesa fin da ora.

• Scadenze ravvicinate sulla trasparenza. Gli obblighi di marcatura dei contenuti generati e l'adeguamento al nuovo divieto sui contenuti abusivi hanno una data più vicina, il 2 dicembre 2026. Per chi offre funzionalità generative, questa è la scadenza più immediata.

• Notifica degli incidenti potenzialmente più semplice. Il Single-Entry Point potrebbe ridurre le segnalazioni duplicate. La sua effettiva portata dipende però dall'iter del Digital Omnibus generale, ancora aperto.

• Incertezza sul fronte dati. Le modifiche a GDPR e cookie sono tra le più controverse e le più lontane da un testo finale. È l'area in cui conviene evitare conclusioni premature.

• Necessità di mappatura interna. Le imprese dovrebbero identificare quali regimi si applicano ai propri sistemi, quali autorità sono coinvolte e quali procedure interne saranno da aggiornare. La semplificazione normativa non elimina il bisogno di governance interna.

7. Che cosa non cambia

Il Digital Omnibus mira a ridurre duplicazioni, disallineamenti e oneri procedurali, ma non elimina la necessità di governance interna. Le organizzazioni dovranno continuare a mappare trattamenti, sistemi, fornitori, incidenti, basi giuridiche, autorità competenti, sistemi di IA e obblighi settoriali applicabili.

La semplificazione dei canali e delle scadenze non sostituisce la responsabilità dell'organizzazione nel dimostrare che i propri processi sono adeguati, proporzionati e verificabili. Un punto unico di notifica, se adottato, può ridurre l'attrito amministrativo, ma non trasforma automaticamente un processo interno debole in una risposta regolatoria solida.

In questo scenario, la semplificazione normativa non riduce il bisogno di evidenza. Al contrario, lo rende più visibile: meno duplicazioni formali significano maggiore pressione sulla qualità delle prove interne, sulla tracciabilità degli artefatti e sulla capacità di dimostrare, senza esporre più dati del necessario, che un processo, un incidente, un dataset o una configurazione esistevano in una determinata forma in un determinato momento.

8. Il contesto internazionale: USA, Regno Unito e Svizzera

Il Digital Omnibus non opera in un vuoto. Le organizzazioni che trattano dati o impiegano sistemi di IA si muovono in un contesto globale in cui le grandi giurisdizioni stanno adottando approcci diversi. Mentre l'Unione europea conferma un modello prescrittivo e basato sul rischio, pur cercando di semplificarlo, Stati Uniti, Regno Unito e Svizzera seguono traiettorie differenti.

Comprendere queste differenze aiuta a valutare i possibili attriti e le aree di interoperabilità con il quadro europeo.

Giurisdizione	Approccio all'AI	Interoperabilità con il Digital Omnibus
USA	Volontario e settoriale: nessuna legge federale orizzontale; framework NIST non vincolante e regole di settore.	Possibili attriti sulla definizione di alto rischio e sui criteri di conformità.
Regno Unito	Modello basato su principi, light-touch: cinque principi applicati dai regolatori di settore esistenti.	Maggiore flessibilità, ma incertezza sul mutuo riconoscimento con il regime UE.
Svizzera	Allineamento GDPR-like sui dati; sull'IA nessuna legge orizzontale, ma ratifica della Convenzione del Consiglio d'Europa e interventi settoriali.	Adeguatezza UE già acquisita da preservare; attenzione alle divergenze tra regolazione dei dati e regolazione dell'IA.

8.1 Stati Uniti: framework volontari e tensione federale-statale

Gli Stati Uniti non dispongono di una legge federale organica sull'intelligenza artificiale. L'impianto resta settoriale e in larga parte volontario: le autorità esistenti applicano le norme di propria competenza anche all'IA, mentre il NIST AI Risk Management Framework fornisce una guida non vincolante per la governance dei sistemi.

Il quadro è reso più complesso da una tensione tra livello federale e livello statale. L'amministrazione in carica ha adottato un orientamento deregolatorio e punta a uno standard federale minimamente oneroso, mentre numerosi Stati hanno legiferato in modo autonomo. Ne risulta un mosaico normativo che può aumentare, anziché ridurre, l'incertezza per le imprese.

Punto di attrito con l'UE

La principale frizione riguarda la definizione di alto rischio. L'approccio europeo classifica ex ante intere categorie di sistemi come ad alto rischio, con obblighi

stringenti; l'approccio statunitense, volontario e settoriale, non fissa una soglia equivalente. Un'organizzazione attiva su entrambi i mercati può quindi dover gestire categorie e obblighi non sovrapponibili.

8.2 Regno Unito: un modello basato su principi

Il Regno Unito ha scelto, almeno in questa fase, di non adottare una legge orizzontale sull'IA. L'AI White Paper del 2023 affida ai regolatori di settore già esistenti, tra cui ICO, FCA, Ofcom, CMA e MHRA, il compito di applicare cinque principi trasversali: sicurezza e robustezza; trasparenza ed esplicabilità appropriate; correttezza; responsabilità e governance; contestabilità e possibilità di ricorso.

È un modello light-touch, orientato a favorire l'innovazione. Il vantaggio è che le imprese dialogano con regolatori già familiari; lo svantaggio è che regolatori diversi possono interpretare gli stessi principi in modo divergente. Una proposta di legge sull'IA è in discussione, ma a metà 2026 non risulta ancora approvata.

Sul fronte dei dati, il Data (Use and Access) Act 2025 ha introdotto riforme allo UK GDPR, incluse modifiche alle decisioni automatizzate. La Commissione europea ha rinnovato nel dicembre 2025 le decisioni di adeguatezza per il Regno Unito, consentendo la prosecuzione dei trasferimenti di dati personali dallo Spazio economico europeo verso il Regno Unito. Anche questo profilo resta da monitorare, perché eventuali divergenze future tra quadro britannico e quadro europeo possono incidere sull'interoperabilità regolatoria.

Punto di attrito con l'UE

La flessibilità britannica offre margini di manovra, ma introduce incertezza sul mutuo riconoscimento. La conformità nel Regno Unito non garantisce automaticamente la conformità nell'UE, soprattutto per obblighi specifici come l'etichettatura dei contenuti generati.

8.3 Svizzera: allineamento sui dati, approccio settoriale sull'IA

La Svizzera presenta un profilo duplice. Sul fronte della protezione dei dati, la nuova Legge federale sulla protezione dei dati, in vigore dal 1° settembre 2023, è stata costruita in allineamento con il GDPR. Questo allineamento ha consentito alla Svizzera

di mantenere la propria posizione di adeguatezza nei confronti dell'UE, riconfermata dalla Commissione europea nel gennaio 2024.

Sul fronte dell'intelligenza artificiale, il Consiglio federale ha deciso il 12 febbraio 2025 di non adottare una legge orizzontale sul modello dell'AI Act europeo. La scelta è invece ratificare la Convenzione sull'IA del Consiglio d'Europa e procedere con interventi settoriali mirati. Un progetto da porre in consultazione è atteso entro la fine del 2026, con attenzione a trasparenza, protezione dei dati, non discriminazione e vigilanza.

Considerati i tempi della procedura legislativa svizzera, l'entrata in vigore di nuove disposizioni orizzontali o settoriali sull'IA richiederà verosimilmente un orizzonte pluriennale. Nel frattempo, per le organizzazioni attive anche nel mercato europeo, il punto centrale resta la capacità di gestire in modo coerente i requisiti UE, svizzeri e contrattuali applicabili.

Punto di attenzione

L'adeguatezza sui dati è un risultato da preservare, non da conquistare. La sfida è evitare che un approccio più leggero e settoriale sull'IA crei, nel tempo, disallineamenti proprio nei punti in cui regolazione dell'IA e protezione dei dati personali si sovrappongono.

9. Glossario essenziale

Termine	Significato
AI Act	Regolamento UE 2024/1689 sull'intelligenza artificiale, basato su un approccio per livelli di rischio.
NIS2	Direttiva UE 2022/2555 sulla sicurezza delle reti e dei sistemi informativi; amplia il perimetro delle infrastrutture critiche.
DORA	Regolamento UE 2022/2554 sulla resilienza operativa digitale del settore finanziario, applicabile dal 17 gennaio 2025.
CER	Direttiva sulla resilienza dei soggetti critici, Critical Entities Resilience.
GDPR	Regolamento UE 2016/679 sulla protezione dei dati personali.

ENISA	Agenzia dell'Unione europea per la cybersicurezza, incaricata di sviluppare il punto unico di notifica.
Trilogo	Negoziato informale tra Commissione, Parlamento e Consiglio per concordare il testo finale di una norma.
Allegato I / III	Elenchi dell'AI Act: l'Allegato III riguarda i sistemi ad alto rischio autonomi; l'Allegato I i sistemi integrati in prodotti già regolati.

10. Cronologia essenziale

Data	Evento
17 gen 2025	DORA diventa pienamente applicabile.
19 nov 2025	La Commissione presenta il Digital Package, comprensivo dei due Omnibus.
11 mar 2026	Si chiude la consultazione pubblica collegata al digital fitness check.
28 apr 2026	Primo trilogo sull'AI Omnibus: nessun accordo, soprattutto per il nodo sui prodotti settoriali.
7 mag 2026	Accordo politico provvisorio sul Digital Omnibus on AI.
2 ago 2026	Data prima della quale i co-legislatori puntano ad adottare formalmente l'AI Omnibus.
2 dic 2026	Termine per l'etichettatura dei contenuti generati e per l'adeguamento al divieto sui contenuti abusivi.
2 dic 2027	Nuova data di applicazione per i sistemi ad alto rischio dell'Allegato III.
2 ago 2028	Nuova data di applicazione per i sistemi ad alto rischio dell'Allegato I.

11. Link e fonti di riferimento

I collegamenti seguenti rimandano a fonti istituzionali e ad analisi utilizzate per la redazione del dossier. Le fonti istituzionali sono da preferire per il dato ufficiale; le analisi di studi legali e testate specializzate aiutano a interpretarne la portata. L'elenco non è esaustivo.

Fonti istituzionali europee

• Commissione europea — pagina ufficiale sul Digital Omnibus / pacchetto digitale — https://digital-strategy.ec.europa.eu/en/policies/digital-omnibus

• Consiglio dell'UE — comunicato sull'accordo per semplificare le regole sull'IA — https://www.consilium.europa.eu/en/press/press-releases/

• Parlamento europeo — comunicato sull'accordo AI Act / app di nudification — https://www.europarl.europa.eu/news/en/press-room

• EUR-Lex — testo dell'AI Act, Regolamento UE 2024/1689 — https://eur-lex.europa.eu/eli/reg/2024/1689/oj

• ENISA — Agenzia dell'Unione europea per la cybersicurezza — https://www.enisa.europa.eu/

Stati Uniti

• NIST — AI Risk Management Framework — https://www.nist.gov/itl/ai-risk-management-framework

• White House — executive order Ensuring a National Policy Framework for AI — https://www.whitehouse.gov/presidential-actions/

Regno Unito

• GOV.UK — AI regulation: a pro-innovation approach — https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach

• ICO — guida su intelligenza artificiale e protezione dei dati — https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/

Svizzera

• Consiglio federale — comunicato sull'approccio alla regolazione dell'IA — https://www.admin.ch/gov/en/start/documentation/media-releases.html

• Ufficio federale di giustizia — adeguatezza UE e protezione dei dati — https://www.bj.admin.ch/bj/en/home/staat/datenschutz/internationales/angemessenheit-ch.html

• IFPDT — autorità federale per la protezione dei dati e la trasparenza — https://www.edoeb.admin.ch/

Convenzioni e standard internazionali

• Consiglio d'Europa — Convenzione quadro sull'intelligenza artificiale — https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

• OCSE — Principi sull'intelligenza artificiale — https://oecd.ai/en/ai-principles

Cybersecurity, IA e protezione dei dati

• EDPB/EDPS — Joint Opinion 2/2026 sul Digital Omnibus — https://www.edpb.europa.eu/

• Google Project Zero — From Naptime to Big Sleep — https://projectzero.google/

• Google Cloud Threat Intelligence — Adversaries Leverage AI for Vulnerability Exploitation and Initial Access — https://cloud.google.com/blog/topics/threat-intelligence/

• Google — A summer of security: empowering cyber defenders with AI — https://blog.google/

Nota: gli indirizzi rimandano alle pagine istituzionali principali; poiché i percorsi dei singoli comunicati possono cambiare nel tempo, in caso di link non più valido si consiglia di cercare il documento per titolo e data sul sito dell'ente competente.

Avvertenza

Documento a finalità divulgative, aggiornato a maggio 2026. Non costituisce consulenza legale. Lo stato dell'iter e i dettagli dei testi sono provvisori e soggetti a modifica fino alla pubblicazione definitiva nella Gazzetta Ufficiale dell'Unione europea. Per applicazioni operative si rinvia ai testi ufficiali e a un parere professionale qualificato.

POSTFAZIONE

Il ritardo strutturale: quando la norma insegue una realtà che corre

La parte precedente del dossier ha descritto un'azione di riordino: l'Unione europea che prova a semplificare, allineare scadenze e rendere più coerenti norme nate in momenti diversi. È un lavoro necessario. Ma proprio perché necessario, rischia di nascondere una domanda più scomoda: che cosa accade quando il diritto riesce a ordinare il quadro esistente, ma il quadro tecnico si è già spostato altrove?

Questa postfazione non aggiunge un nuovo capitolo normativo. È una divagazione conclusiva, una lente laterale. Serve a guardare il Digital Omnibus da un'altra angolatura: come sintomo di un problema più profondo, il divario tra il tempo della norma e il tempo del software.

La tesi è semplice: anche nella sua versione più ordinata, il corpus digitale europeo si muove su una scala temporale diversa rispetto alla realtà che vuole governare. Non è un difetto specifico del Digital Omnibus. È una tensione strutturale. Il diritto procede per consultazioni, proposte, negoziati, triloghi, revisioni, recepimenti e scadenze differite. Il software, invece, muta per aggiornamenti, fork, patch, modelli rilasciati, catene di dipendenza, vulnerabilità scoperte e sfruttate in tempi sempre più brevi.

Che cosa è cambiato nella scoperta delle vulnerabilità

Fino a poco tempo fa, individuare una falla sfruttabile in un sistema reale richiedeva competenze rare e tempi lunghi. Questa premessa, su cui poggiano implicitamente molti obblighi normativi, è oggi meno stabile. Strumenti basati su modelli linguistici di grandi dimensioni sono in grado di leggere e ragionare su ampie basi di codice, guidare test mirati e, in casi documentati, concatenare passaggi tecnici che trasformano un difetto in un attacco funzionante.

L'aspetto più rilevante, dal punto di vista regolatorio, è la capacità di individuare falle su misura: non solo vulnerabilità note e catalogate, ma errori logici, configurazioni marginali, assunzioni implicite o componenti legacy che sfuggono alle categorie tradizionali della pianificazione del rischio.

La sicurezza aziendale tende spesso a concentrarsi su ciò che è visibile, formalizzato e periodicamente controllato. Ma gli ambienti più esposti possono essere proprio

quelli laterali: vecchie integrazioni, librerie dimenticate, configurazioni temporanee diventate permanenti, automatismi interni che nessuno ha più riesaminato. Sono zone grigie. E le zone grigie sono precisamente ciò che una capacità automatizzata di esplorazione può rendere improvvisamente rilevante.

I fatti che rendono concreto il divario

Alcuni sviluppi pubblici, riconducibili al periodo 2024-2026, aiutano a capire perché il problema non sia teorico. Gli esempi che seguono non devono essere letti come prova che ogni vulnerabilità sarà scoperta o sfruttata automaticamente da sistemi di IA, ma come segnali di una compressione dei tempi e di un ampliamento delle capacità disponibili.

• La capacità dichiarata dai produttori stessi. Alcuni produttori e gruppi di ricerca hanno documentato sistemi di IA capaci di analizzare basi di codice complesse, individuare vulnerabilità reali e supportare attività di verifica tecnica. Il caso Big Sleep/Project Zero di Google mostra come un agente di sicurezza possa contribuire alla scoperta o alla prevenzione dello sfruttamento di vulnerabilità, inclusi casi in cui threat intelligence e analisi automatizzata sono state combinate per ridurre la finestra di esposizione.

• L'uso dell'IA in scenari offensivi reali. Report di threat intelligence del 2026 indicano un uso crescente dell'IA nei workflow offensivi, inclusi riconoscimento, sviluppo di strumenti, supporto allo sfruttamento di vulnerabilità e automazione operativa. Anche quando attribuzione, successo dell'attacco e grado di autonomia restano oggetto di cautela, la soglia operativa rilevante è stata superata: l'IA non è più soltanto strumento difensivo o di laboratorio.

• La compressione dei tempi. Il percorso dal concetto all'exploit funzionante può ridursi drasticamente quando un modello è usato per orientare ricerca, test e validazione. La finestra tra divulgazione pubblica di una falla e sfruttamento di massa tende a restringersi. È un ordine di grandezza difficilmente compatibile con cicli normativi misurati in anni.

• La natura a duplice uso degli strumenti. Gli stessi strumenti che aiutano i difensori a trovare vulnerabilità e verificare patch possono aiutare gli attaccanti a ridurre tempi, costi e competenze necessarie. La tecnologia non è buona o cattiva in sé: dipende dall'uso, dal contesto e dall'autorizzazione.

Questi esempi vanno letti con prudenza. L'esistenza di capacità avanzate non significa che ogni organizzazione sia esposta allo stesso livello, né che la regolazione diventi irrilevante. Significa piuttosto che la distanza tra emersione tecnica del rischio e aggiornamento formale delle categorie normative può diventare molto ampia.

Perché la norma fatica a stare al passo

Il disallineamento nasce da tre caratteristiche della regolazione, nessuna delle quali è di per sé sbagliata.

La prima è il tempo. Un regolamento europeo richiede anni tra proposta, negoziato, adozione e applicazione. L'AI Act è entrato in vigore nel 2024 e i suoi obblighi sull'alto rischio, persino dopo il rinvio, arrivano tra fine 2027 e metà 2028. Una capacità tecnica, invece, può diffondersi in mesi.

La seconda è la classificazione statica. L'approccio europeo definisce categorie di rischio in anticipo. Ma una vulnerabilità specifica di una configurazione marginale non appartiene necessariamente a una categoria prevista. È, per costruzione, l'eccezione che lo schema non aveva visto.

La terza è l'oggetto regolato. Le norme esaminate disciplinano soprattutto sistemi, fornitori, deployer, soggetti obbligati e procedure. La capacità di scoprire vulnerabilità, però, può risiedere in strumenti generici e ampiamente disponibili. Lo stesso modello può essere usato per audit legittimi o per attività illecite. Una norma di prodotto cattura solo in parte questa ambivalenza.

Il punto, in una frase

Il Digital Omnibus rende più ordinato e coerente l'impianto esistente, ma non ne modifica la velocità. Finché il rischio si sposta più rapidamente di quanto il diritto riesca a riclassificarlo, conformità formale e sicurezza reale possono divergere: si può essere pienamente conformi e, allo stesso tempo, esposti a una falla che nessuna categoria normativa aveva previsto.

Una lettura equilibrata

Sarebbe però sbagliato concludere che la norma sia inutile solo perché arriva più lentamente della tecnologia. La regolazione non nasce per prevedere ogni singola vulnerabilità. Serve a distribuire responsabilità, fissare obblighi minimi, imporre

processi, rendere verificabile la governance e costruire un linguaggio comune tra imprese, autorità e cittadini.

Chi sottolinea i limiti della regolazione osserva che un quadro statico e lento non può governare da solo un rischio dinamico e veloce. Il pericolo è scambiare la conformità documentale per sicurezza effettiva. In questa lettura, la vera resilienza dipende da capacità operative: rilevamento continuo, correzione rapida, monitoraggio della catena di fornitura, test ricorrenti, difese capaci di muoversi anch'esse a velocità di macchina.

Chi difende il valore della regolazione ricorda invece che norme come NIS2 e DORA non pretendono di prevedere ogni falla. Impongono processi di gestione del rischio, controllo dei fornitori, continuità operativa, notifica degli incidenti e responsabilità organizzativa. In un mondo più veloce, questi processi possono diventare ancora più importanti, perché creano l'infrastruttura entro cui le difese tecniche possono funzionare.

Le due letture non si escludono. La conclusione più solida è che norma e capacità tecnica svolgono funzioni diverse. La norma fissa obblighi e responsabilità durevoli; la capacità tecnica affronta la minaccia nel momento in cui si manifesta. Il rischio da evitare è scambiare l'una per l'altra: credere che l'adempimento normativo basti a garantire la sicurezza, oppure che la competenza tecnica renda superflua la responsabilità giuridica.

Il Digital Omnibus migliora il primo versante: ordina, allinea, riduce duplicazioni, rende più leggibile il quadro. Il secondo versante richiede invece strumenti, competenze e prontezza operativa che nessuna semplificazione normativa, da sola, può fornire.