DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La proposta legislativa del «Digital Omnibus Act»

Giugno 2026

Giuseppe Proietti, Lener & Partners

Giuseppe Proietti, Lener & Partners

Studio legale

Lener & Partners

1. La ulteriormente «nuova» politica digitale europea

Il 19 novembre 2025, la Commissione Europea ha presentato un articolato pacchetto legislativo, comunemente noto come *Digital Omnibus Act* e composto principalmente dalle proposte di regolamento COM (2025) 836 e COM (2025) 837. L'iniziativa si inserisce nel più ampio contesto della *Data Union Strategy* e della strategia per la competitività del mercato unico digitale europeo. A questa architettura normativa si somma un insieme di norme per la «sovranità tecnologica», più volte rinviata [1].

La logica di fondo della proposta del *Digital Omnibus Act* è quella di una rivisitazione del quadro normativo europeo nel settore digitale: l'insieme delle norme digitali adottate negli anni immediatamente precedenti - dall'*AI Act* (2024) al *Data Act* (2023), dal GDPR alla Direttiva *e-Privacy*, passando per NIS2, DORA e il regolamento eIDAS, ha generato, nella sua applicazione pratica - laddove effettivamente implementata - una stratificazione normativa di notevole complessità, volendo usare un lessico garbato. È stata quindi ricavata l'ovvia considerazione che una simile complessità si andrebbe a tradurre in oneri significativi per le imprese, frammentazione interpretativa tra gli Stati membri e, talvolta, sovrapposizioni tra gli obblighi derivanti dai diversi atti legislativi. Si potrebbe aggiungere un ulteriore effetto: utenti o consumatori inconsapevoli, o quantomeno confusi, circa i loro diritti e doveri.

Sicché, la Commissione UE dichiara espressamente che la proposta non mira a modificare gli obiettivi sostanziali di tutela dei diritti fondamentali, né ad abbassare gli standard di protezione già consolidati, bensì a semplificare le procedure, chiarire le definizioni e razionalizzare il sistema degli obblighi in capo a imprese e p.a. La base giuridica principale dell'intervento è individuata nel sempre invocato articolo 114 del Trattato sul Funzionamento dell'Unione Europea (TFUE) relativo al funzionamento del mercato interno, con ulteriori richiami a disposizioni di settore a seconda dei singoli atti che verrebbero riformati.

1 Il pacchetto di norme dovrebbe comprendere proposte legislative nell'ambito di infrastrutture digitali, tra cui il cloud e l'AI Development Act (CAIDA) per il rafforzamento dello sviluppo di data center. All'interno di questo "pacchetto" viene incluso anche l'*AI act* e il *Data Act*. Questa iniziativa è stata più volte rinviata e l'ultima volta è avvenuto a seguito di un monito da parte dell'ambasciatore statunitense in UE che ha avvertito circa il fatto che una simile iniziativa di tipo protezionistico avrebbe potuto mettere a rischio accordi commerciali con gli USA.

vedi l'articolo online

Il nuovo quadro normativo abbraccia un raggio d'azione estremamente ampio e altrettanto elaborato: interviene sul neonato *Data Act* (che dovrebbe costituire il fulcro del nuovo assetto normativo), sul Regolamento Generale sulla Protezione dei Dati (GDPR), sulla Direttiva *ePrivacy*, sulla Direttiva NIS2 e sul Regolamento DORA, così come sul Regolamento eIDAS, sulla Direttiva CER e sul famosissimo e recentissimo Regolamento sull'intelligenza artificiale (*AI Act*).

Questa ulteriore iniziativa legislativa europea abroga, tra gli altri, il Regolamento sulla libera circolazione dei dati non personali (FFDR), il recente *Data Governance Act* (le cui disposizioni più importanti verrebbero assorbite nel *Data Act*), la Direttiva *Open Data* e il Regolamento *Platform-to-Business* del 2019(P2B). L'ambizione dichiarata è quella di creare un quadro normativo più coerente, riducendo duplicazioni e conflitti tra le norme vigenti, e di adottare un approccio che la Commissione UE stessa qualifica come un "primo passo" nell'ambito di un processo di semplificazione destinato a proseguire con ulteriori strumenti.

La Commissione, in pari data, ha adottato una comunicazione "La strategia per l'Unione dei dati sbloccare i dati per l'IA".

Nella Comunicazione si fa menzione di una *strategia per l'Unione dei dati* con cui si sposta l'attenzione «dalle norme ai risultati», facendo presagire, forse, all'ambizione di risultati pratici.

Quindi, stando a tale Comunicazione, l'UE agirà nel quadro di tre settori prioritari:

(i) ampliamento dell'accesso ai dati per l'IA, attraverso iniziative quali i *laboratori di dati* che offrono servizi di pseudonimizzazione affidabili e mettono in comune le risorse in termini di dati tra i soggetti pubblici e privati per fornire alle imprese e ai ricercatori serie di dati di alta qualità[2];

2 A pagina 5 della Comunicazione si legge che: «I laboratori di dati fungeranno da strutture di servizio specializzate atte a garantire ambienti sicuri, strumenti pratici e assistenza specialistica per la messa in comune, la cura, la pseudonimizzazione e l'anonimizzazione dei dati. Essi aiuteranno le imprese, in particolare le PMI, a trasformare i dati in risorse utilizzabili per l'addestramento dell'IA, al contempo preservandone il controllo. Tali sforzi andranno di pari passo con la strategia per l'IA applicata, garantendo che la disponibilità di dati favorisca direttamente la diffusione e l'innovazione dell'IA in tutte le industrie e i settori pubblici. In secondo luogo, la Commissione intensificherà gli sforzi facendo leva su fattori abilitanti orizzontali: chiarezza giuridica per la messa in comune dei dati, norme per la qualità dei dati e investimenti nelle capacità di dati sintetici, garantendo diffusione, affidabilità e

(ii) razionalizzazione delle norme in materia di dati, al fine di facilitare la condivisione dei dati per le imprese e i ricercatori, compresa la riforma del consenso ai cookie per renderlo meno laborioso e tutelare al contempo i diritti[3];

(iii) rafforzamento della posizione globale dell'UE sui flussi internazionali di dati, affrontando gli ostacoli ingiustificati agli scambi in modo che le imprese europee possano competere in condizioni di parità a livello globale.

Tale "strategia" europea fa seguito a quella del 2020, denominata "strategia europea per i dati – Plasmare il futuro digitale dell'Europa" che, probabilmente non ha dato vita a risultati molto entusiasmanti. Tuttavia, la Commissione UE la rammenta, considerandola una "strategia" che «*ha posto le fondamenta giuridiche e istituzionali per un mercato unico dei dati sicuro ed equo. L'obiettivo era sbloccare il potenziale dei dati per l'innovazione e la crescita, tutelando al contempo i diritti*». L'avvento dell'IA generativa, però, viene precisato, ha reso evidente la necessità che l'UE vada oltre le sue attuali fondamenta [4].

2. Le proposte legislative del *Digital Omnibus*: il Consolidamento del *Data Acquis*

Uno dei pilastri più significativi della proposta, come si è visto, è la razionalizzazione del quadro normativo europeo in materia di dati attraverso un processo di consolidamento normativo che si incentra sul *Data Act*. La proposta, infatti, prevede l'integrazione, all'interno del recentissimo *Data Act* (Regolamento UE 2023/2854), delle disposizioni essenziali oggi contenute in atti distinti.

In primo luogo, viene prevista l'abrogazione del **Regolamento sulla libera circolazione dei dati non personali** (FFDR), con la contestuale trasposizione dei suoi principi fondamentali - in particolare il divieto di localizzazione ingiustificata dei dati non personali - nella struttura del *Data Act*. Tale abrogazione viene motivata per il fatto che le disposizioni del FFDR sarebbero ormai da ricomprendersi nella corni-

sostenibilità a lungo termine in tutti i settori». Nella successiva pagina 11 viene riportato un esempio pratico di "laboratorio di dati".

3 A pagina 4 della Comunicazione si legge che: «per sbloccare l'innovazione, è necessario che l'UE semplifichi le norme relative all'accesso ai dati e al loro utilizzo».

4 Cfr. Comunicazione cit., pag. 2.

vedi l'articolo online

ce più ampia e aggiornata del *Data Act*.

In secondo luogo, la proposta prevede l'abrogazione anche dell'altrettanto recente **Data Governance Act (DGA)** e l'assorbimento delle sue disposizioni principali nel *Data Act*. Ciò riguarda in particolare la disciplina sui servizi di intermediazione dei dati (*data intermediation services*) e alle organizzazioni di altruismo dei dati (*data altruism organisations*). Viene promosso un regime semplificato per i fornitori di servizi di intermediazione con l'obiettivo dichiarato di favorire modelli di business praticabili per gli intermediari. Viene perciò proposta una legislazione con obblighi più "flessibili" per gli intermediari e la possibilità, per questi ultimi, di svolgere parallelamente anche una diversa attività d'impresa, purché i due servizi rimangano separati dal punto di vista funzionale. Per le organizzazioni di altruismo dei dati, vengono mantenuti i principi fondamentali di neutralità e separazione funzionale, ma verrebbero razionalizzate le procedure di registrazione e gli obblighi di rendicontazione.

In terzo luogo, si prevede l'abrogazione della direttiva **Open Data** e la creazione di un unico capitolo nel *Data Act* dedicato al riutilizzo dei dati e dei documenti detenuti dagli enti pubblici. In un capo del *Data Act* vengono consolidati i principi di apertura, trasparenza e accesso equo, con disposizioni specifiche sulle condizioni applicabili al riutilizzo, sulle eventuali tariffe e sui formati aperti e leggibili meccanicamente. Viene poi introdotto un *single information point* per facilitare l'individuazione e l'accesso ai dataset pubblici disponibili.

Sul fronte della condivisione dei dati tra imprese e pubbliche amministrazioni (Business-to-Government, B2G), la proposta opera un significativo restringimento dell'ambito applicativo: l'obbligo di condivisione dei dati da parte delle imprese verso le autorità pubbliche viene limitato ai soli casi di emergenza pubblica, abbandonando la formulazione precedente che faceva riferimento a un più generico "necessità eccezionali". Tale scelta risponderebbe all'esigenza di non gravare le imprese con obblighi di condivisione difficilmente prevedibili.

Viene inoltre introdotto un meccanismo specifico per la protezione dei segreti commerciali in caso di richieste di condivisione dei dati: i detentori di dati potranno rifiutare la condivisione qualora sussista un elevato rischio che i segreti commerciali vengano acquisiti illecitamente da entità di paesi terzi, in particolare qualora non siano in vigore accordi internazionali adeguati che garantiscano un livello equivalente di protezione rispetto a quello europeo.

Viene proposta una rimodulazione di norme riguardanti gli *smart contracts* per l'esecuzione degli accordi di condivisione dei dati a causa della difficoltà di applicazione pratica delle previsioni normative vigenti.

Infine, la proposta estende i regimi di favore già previsti per le piccole e medie imprese (PMI) anche alle cosiddette "small mid-caps" (SMC), con l'obiettivo di sostenere le imprese in fase di crescita senza gravare eccessivamente sui loro processi di conformità.

La proposta prevede l'abrogazione del Regolamento (UE) 2019/1150 **Platform-to-Business**, relativo alla promozione dell'equità e della trasparenza per gli utenti commerciali dei servizi di intermediazione online (P2B). La motivazione addotta dalla Commissione è che le disposizioni del regolamento sono ormai ampiamente sovrapposte con normative successive di portata più ampia, in particolare dal Regolamento sui mercati digitali (DMA) e dal Regolamento sui servizi digitali (DSA), che disciplinano in modo più completo le relazioni tra le piattaforme e i loro utenti commerciali. In altri termini, si sono venute a generare delle vere e proprie antinomie.

3. Le modifiche al GDPR e alla direttiva e-Privacy

La proposta interviene in modo mirato su alcune disposizioni del GDPR (Regolamento UE 2016/679) e della Direttiva e-Privacy (Direttiva 2002/58/CE), con l'obiettivo dichiarato di chiarire il testo normativo, ridurre gli oneri e adattare il quadro alle sfide dell'economia digitale e dell'intelligenza artificiale.

La ridefinizione della **nozione di dato personale** rappresenta forse la modifica più dibattuta[5]. La propo-

5 Forti critiche sono state sollevate sulla modifica della definizione di dato personale. Si ritiene che l'approccio "soggettivo" proposto dalla Commissione creerebbe scappatoie sistemiche. In altri termini, un titolare del trattamento potrebbe affermare di non disporre di mezzi ragionevoli per identificare un individuo, escludendo così i dati dalla tutela del GDPR, anche in casi in cui un soggetto terzo o la stessa autorità di controllo potrebbero agilmente procedere all'identificazione. La critica si estende alla proposta di delegare alla Commissione il potere di definire, tramite atti di esecuzione, quali tecniche di pseudonimizzazione rendano i dati non personali per determinate categorie di entità. Le critiche sono mosse dall'organizzazione NOYB nella prima versione del documento "Digital Omnibus. First Analysis of Select GDPR and ePrivacy Proposals by the Commission". Critiche sono state sollevate

sta introduce un chiarimento, ispirato alla giurisprudenza della Corte di Giustizia dell'Unione Europea, secondo cui un dato deve essere considerato personale soltanto se l'entità che lo tratta dispone di mezzi che rendono ragionevolmente probabile l'identificazione della persona fisica a cui si riferisce. In altri termini, la qualificazione di un dato come personale diviene relativa al soggetto che lo tratta: se un titolare del trattamento non dispone e non può ragionevolmente acquisire i mezzi per identificare l'interessato, quel dato non è "personale" per quell'entità. Viene altresì introdotto un nuovo articolo del GDPR, che attribuisce alla Commissione il potere di adottare atti di esecuzione per specificare i criteri e le tecniche di pseudonimizzazione alla luce dei quali i dati non devono essere considerati personali per talune categorie di soggetti.

Relativamente alla **pseudonimizzazione e all'anonimizzazione**, la proposta introduce meccanismi, che devono essere elaborati dalla Commissione e dal Comitato europeo per la protezione dei dati, volti a offrire maggiore certezza agli operatori su quando i dati pseudonimizzati cessino di essere qualificabili come dati personali per determinati soggetti, tenuto conto dello stato dell'arte delle tecnologie di re-identificazione.

In materia di **diritto di accesso**, la proposta introduce la possibilità per il titolare del trattamento di rifiutare o limitare le richieste di accesso qualora si possa ritenere che ci sia un abuso da parte degli interessati per finalità diverse rispetto alla protezione dei loro dati personali[6].

Sulla **informativa da parte del titolare del trattamento** ai sensi dell'art. 13 GDPR, viene escluso l'obbligo se vi sono ragionevoli motivi per ritenere che l'interessato già disponga delle informazioni, a meno che il titolare del trattamento non trasmetta i dati ad altri destinatari o categorie di destinatari, trasferisca i dati a un paese terzo, effettui un processo decisionale automatizzato i se ci possa essere un rischio elevato per i diritti dell'interessato.

Sul fronte delle **notifiche di violazioni dei dati personali** (*data breach*), la soglia per l'obbligo di notifica all'autorità di controllo viene innalzata. Infatti, la comunicazione diventerebbe obbligatoria esclusivamente in caso di violazioni che presentino un "rischio elevato" per i diritti e le libertà degli interessati, superando così la formulazione attuale. Il termine per la notifica viene esteso da 72 a 96 ore.

Le proposte di modifica alla disciplina delle **valutazioni d'impatto sulla protezione dei dati** (DPIA, art. 35 GDPR) prevedono la creazione di liste comuni a livello UE, elaborate dall'EDPB, delle tipologie di trattamento che richiedono obbligatoriamente una DPIA e di quelle che ne sono esenti. La finalità è quella di armonizzare le prassi nazionali, attualmente frammentate, e di ridurre l'incertezza giuridica per gli operatori che operano in più giurisdizioni.

Per quanto riguarda l'**IA,** vengono discusse le **basi giuridiche per il trattamento**, focalizzandosi su quella del legittimo interesse (art. 6, par. 1, lett. f, GDPR) e del consenso, in modo che sia individuata quella più corretta per il trattamento di dati personali nell'ambito dello sviluppo e dell'operatività dei sistemi di IA. Viene discussa e proposta una "deroga" specifica per il trattamento di categorie particolari di dati (c.d. dati sensibili, art. 9 GDPR) se il trattamento avviene nell'ambito della fase di addestramento dei modelli di IA e il titolare abbia adottato misure tecniche e organizzative appropriate per minimizzare tale trattamento e prevenirne gli effetti discriminatori[7].

Sul piano della disciplina dei **processi decisionali automatizzati** (art. 22 GDPR), la proposta introduce chiarimenti interpretativi volti a precisare la portata del principio di "necessità" in relazione all'esecuzione di un contratto, con l'obiettivo di ridurre l'incertezza applicativa emersa in sede di supervisione e nella prassi delle imprese.

sul tema anche nella Joint Opinion 2/2026 dell'EDPB e EDPS on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), consultabile al sito www.edpb.europa.eu.

6 Una proposta di modifica che ha già ricevuto critiche poiché si ritiene che la restrizione del diritto di accesso ai soli fini di protezione dei dati personali sia contraria alla giurisprudenza della Corte di Giustizia, la quale riconosce il diritto di accesso come uno strumento autonomo e non limitabile alle sole finalità di privacy. Tale diritto viene esercitato in molti contesti pratici per scopi distinti come la raccolta di prove in controversie di lavoro, la verifica di decisioni automatizzate, la tutela di interessi legali e la sua limitazione aggraverebbe significativamente lo squilibrio di potere tra titolari del trattamento e interessati. Critiche sempre mosse dall'organizzazione NOYB nella prima versione del documento *Digital Omnibus. First Analysis of Select GDPR and ePrivacy Proposals by the Commission*.

7 Sull'uso del legittimo interesse come base giuridica per lo sviluppo e l'operatività dei sistemi di IA, l'EDPB e l'EDPS, nella Joint Opinion n. 2/2026, riconoscono che tale base giuridica possa, in linea di principio, trovare applicazione, ma rilevano che il bilanciamento tra l'interesse del titolare e i diritti degli interessati deve essere condotto caso per caso e non può essere presunto in modo automatico. Le due autorità chiedono che venga comunque garantito agli interessati un diritto di opposizione incondizionato in tutti i casi in cui il trattamento si fondi sul legittimo interesse.

Per la direttiva **e-Privacy** e la regolamentazione dei cookie la proposta interviene trasferendo al GDPR la disciplina applicabile sull'accesso e memorizzazione di informazioni sui dispositivi terminali degli utenti qualora tali operazioni comportino il trattamento di dati personali. La Direttiva e-Privacy, dunque, continuerebbe ad applicarsi, in modo del tutto residuale, ai casi in cui l'accesso al dispositivo terminale non comporti il trattamento di dati personali.

Per contrastare il fenomeno della cosiddetta *stanchezza da consenso*, la proposta introduce l'obbligo per i titolari del trattamento di rispettare le preferenze degli utenti espresse attraverso segnali automatizzati e leggibili meccanicamente, inclusi quelli trasmessi tramite le impostazioni del browser. In questo modo, l'utente potrà configurare una sola volta le proprie preferenze sulla privacy e vederle rispettate sull'insieme dei siti visitati, senza dover fare fronte a singole richieste di consenso per ciascun servizio. Il titolare è obbligato a rispettare tali segnali automatizzati per un periodo minimo prima di poter riproporre una richiesta di consenso. La proposta introduce altresì la previsione di finalità di trattamento a "rischio limitato" per le quali il consenso è presunto o non necessario, nell'ottica di ridurre la frequenza complessiva delle richieste.

4. Il *Single-entry point* per la notifica degli incidenti di sicurezza

Un altro pilastro rilevante della proposta riguarda la notifica degli incidenti di sicurezza informatica. Attualmente, le imprese che operano in settori regolamentati si trovano ad affrontare obblighi di notifica sovrapposti derivanti da diverse normative: la recente Direttiva NIS2 (recepita in Italia il 4 settembre 2024 con il d.lgs. n. 138), il GDPR, il recente Regolamento DORA, il Regolamento eIDAS e la Direttiva CER prevedono ciascuno proprie procedure, destinatari e tempistiche per la comunicazione degli incidenti alle autorità competenti, creando così un ulteriore dedalo per gli operatori.

La proposta vuole introdurre, quindi, un ***Single-entry point* (SEP)** sviluppato e gestito dall'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA), attraverso il quale le imprese potranno adempiere simultaneamente a tutti i propri obblighi di notifica, indipendentemente dalla normativa applicabile. Il sistema si basa sul principio *report once, share many*: il soggetto notifica l'incidente una sola volta attraverso il portale unico, e l'ENISA provvede a distribuire le informazioni pertinenti alle diverse autorità competenti. La proposta prevede una fase pilota per testare l'affidabilità e l'interoperabilità del sistema prima della sua effettiva operabilità, con la Commissione che valuta e certifica il raggiungimento degli standard di sicurezza e funzionalità richiesti.

Il SEP rappresenta una soluzione di razionalizzazione degli oneri amministrativi particolarmente significativa per gli operatori che operano in settori ad alta regolamentazione, come quello finanziario, energetico o delle infrastrutture critiche, dove la sovrapposizione degli obblighi di notifica è più evidente.

5. Interventi specifici in materia di Intelligenza Artificiale: la proposta "Digital Omnibus on AI"

In parallelo alla proposta di semplificazione del quadro normativo digitale generale, la Commissione ha presentato un distinto ma connesso documento, volto a modificare il Regolamento sull'intelligenza artificiale (*AI Act*, Regolamento UE 2024/1689) e il Regolamento (UE) 2018/1139 in materia di sicurezza dell'aviazione. Tale proposta - comunemente denominata **"Digital Omnibus on AI"** - risponde alle difficoltà di attuazione dell'AI Act emerse già nei primissimi mesi successivi all'entrata in applicazione delle sue disposizioni. Tra i problemi che sono stati rilevati si legge: i ritardi nella designazione delle autorità nazionali competenti; le lacune nella disponibilità di norme armonizzate e specifiche comuni alle quali i fornitori di sistemi ad alto rischio devono conformarsi; la frammentazione della *governance* a livello nazionale; e le incertezze interpretative sull'interazione dell'*AI Act* con altri atti normativi, in particolare con il GDPR.

Le principali misure di semplificazione:

proroga per l'applicazione degli obblighi relativi ai sistemi di IA ad alto rischio costituisce una delle misure più significative. La proposta collega l'entrata in applicazione delle norme per specifiche categorie di sistemi alla disponibilità effettiva di standard armonizzati, specifiche comuni o linee guida della Commissione. Al contempo, vengono fissate date improrogabili per garantire la certezza del diritto: il 2 dicembre 2027 per i sistemi rientranti nell'Allegato III dell'*AI Act* (sistemi di IA ad alto rischio in ambiti come l'istruzione, l'occupazione, i servizi essenziali e l'applicazione della legge) e il 2 agosto 2028 per i sistemi rientranti nell'Allegato I (sistemi soggetti a normative settoriali di sicurezza dei prodotti). Viene contestualmente prevista una "clausola di salvaguardia" (*grandfathering clause*) per i sistemi già immessi sul mercato, con aggiustamenti della data di *cut-off*.

La *governance* e la vigilanza centralizzata dell'AI Office vengono potenziate. Viene introdotto un meccanismo di competenza esclusiva dell'Ufficio per l'IA (AI Office) per la supervisione dei sistemi di IA basati su modelli di IA per finalità generali (General Purpose AI Model, GPAI) nel caso in cui il fornitore del modello sia anche il fornitore del sistema di IA, nonché per i sistemi di IA integrati in piattaforme online di dimensioni molto elevate (VLOP) o motori di ricerca molto grandi (VLOSE). La proposta introduce altresì un meccanismo per l'adozione di atti di esecuzione della Commissione che disciplinino le procedure, i poteri investigativi e le misure correttive dell'AI Office, con richiamo alle garanzie procedurali previste dal Regolamento (UE) 2019/1020 sulla vigilanza del mercato.

La semplificazione degli obblighi per PMI e *small mid-caps* viene realizzata attraverso l'estensione dei regimi agevolati già previsti per le piccole e medie imprese alle imprese di dimensioni intermedie (piccole imprese a media capitalizzazione). Ciò si traduce in una documentazione tecnica semplificata, in un regime di sanzioni proporzionato e in un accesso facilitato alle sandbox regolatorie.

La revisione dell'obbligo "alfabetizzazione" rappresenta una delle modifiche più controverse sul piano dei principi. L'obbligo orizzontale, oggi posto in capo ai fornitori e agli utilizzatori (*deployer*) di sistemi di IA, di garantire un adeguato livello di alfabetizzazione IA del proprio personale, viene trasformato in un dovere di promozione e incoraggiamento in capo alla Commissione europea e agli Stati membri. Rimangono obblighi formativi specifici per i *deployer* di sistemi ad alto rischio, ma l'impostazione generale si orienta verso un approccio di sensibilizzazione diffusa e centralizzata piuttosto che un obbligo individuale[8].

La base giuridica per la correzione dei *bias* algoritmici viene disciplinata attraverso l'introduzione di un nuovo articolo 4-*bis* nell'*AI Act* che consentirebbe l'utilizzo di dati personali particolari.

8 Si tratta di un altro passaggio fortemente (e giustamente) criticato da EDPB ed EDPS nel parere congiunto citato. Gli enti sottolineano che la consapevolezza dei rischi e delle opportunità dell'IA da parte di coloro che operano con i sistemi - tanto i fornitori quanto i *deployer* - è un presidio fondamentale per la protezione dei diritti delle persone. Ridurre tale obbligo a un generico "incoraggiamento" da parte di Commissione e Stati membri rischia di svuotarne il contenuto pratico. Si può aggiungere a quanto riferito dai due enti che l'educazione digitale e l'alfabetizzazione costituiscono due pilastri fondamentali per una corretta attuazione delle trasformazioni tecnologiche in corso. Pilastri che dimostrano come il diritto può aiutare a governare questi processi, ma non costituisce affatto la soluzione di ogni innovazione.

Tale disposizione consente, quindi, in via eccezionale e con rigorose garanzie tecniche e organizzative, il trattamento di categorie particolari di dati personali (dati biometrici, etnici, sanitari, etc.) per la rilevazione e la correzione delle "distorsioni" nei sistemi di IA che potrebbero portare a effetti discriminatori[9]. Le garanzie richieste includono la pseudonimizzazione dei dati, la limitazione tecnica dell'accesso, la cancellazione dei dati personali al termine delle operazioni di correzione e la documentazione dell'intero processo.

Le modifiche agli **obblighi di registrazione** prevedono l'eliminazione dell'obbligo di registrazione nella banca dati UE per i sistemi IA che, pur rientrando nelle categorie ad alto rischio dell'Allegato III, si ritenga non producano rischi significativi ai sensi dell'art. 6, par. 3 dell'*AI Act*.

Una enfasi particolare viene posta sul **potenziamento delle *sandbox* regolatorie**, da attuare attraverso l'estensione delle possibilità di sperimentazione regolata, ossia con la creazione di una sandbox a livello UE, centralizzata e gestita dall'*AI Office*, a partire dal 2028, e ampliando la possibilità di effettuare test in condizioni reali (*real-world testing*) anche al di fuori delle sandbox, per determinate categorie di sistemi, nel rispetto di condizioni specifiche.

Per i fornitori di sistemi di IA generativa soggetti agli **obblighi di marcatura** di cui all'articolo 50, paragrafo 2, del regolamento (UE) 2024/1689, i quali hanno già immesso i loro sistemi sul mercato prima del

9 Si legge, al considerando 6 che: «Il rilevamento e la correzione delle distorsioni costituiscono un interesse pubblico rilevante in quanto proteggono le persone fisiche dagli effetti negativi delle distorsioni, compresa la discriminazione. La discriminazione potrebbe derivare dalla distorsione nei modelli e nei sistemi di IA diversi dai sistemi di IA ad alto rischio, per i quali il regolamento (UE) 2024/1689 fornisce già una base giuridica che autorizza il trattamento di categorie particolari di dati personali ai sensi dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio. Poiché la discriminazione potrebbe derivare anche da altri sistemi e modelli di IA, è opportuno che il regolamento (UE) 2024/1689 fornisca una base giuridica per il trattamento di categorie particolari di dati personali anche da parte dei fornitori e dei deployer di altri sistemi e modelli di IA, nonché dei deployer di sistemi di IA ad alto rischio. La base giuridica è stabilita in conformità dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679, dell'articolo 10, paragrafo 2, lettera g), del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio e dell'articolo 10, lettera a), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, i quali forniscono una base giuridica che consente, ove necessario per il rilevamento e la rimozione di distorsioni, il trattamento di categorie particolari di dati personali da parte dei fornitori e dei deployer di tutti i sistemi e modelli di IA, fatte salve le garanzie adeguate che integrano il regolamento (UE) 2016/679, il regolamento (UE) 2018/1725 e la direttiva (UE) 2016/680, a seconda dei casi».

vedi l'articolo online

2 agosto 2026, viene proposto un periodo transitorio di sei mesi per adeguare le loro pratiche.

6. La Posizione del Parlamento Europeo

Il Parlamento europeo ha delineato, già nelle risoluzioni adottate nell'autunno del 2025, i principi fondamentali ai quali intende ancorare il proprio contributo al processo legislativo sul Digital Omnibus. In particolare, nelle risoluzioni dell'11 settembre 2025 e del 25 novembre 2025, l'istituzione ha sottolineato che la semplificazione normativa è un obiettivo legittimo e necessario, ma non può essere perseguita a scapito della coerenza del quadro giuridico fondamentale dell'UE, della tutela dei diritti digitali dei cittadini europei e della protezione dei consumatori. Il Parlamento ha altresì ribadito l'importanza di condurre valutazioni di impatto approfondite per tutte le proposte legislative, sottolineando che la Commissione ha presentato il Digital Omnibus senza un'apposita valutazione d'impatto separata, scelta contestata da più parti sia in termini di metodo che di sostanza.

L'istituzione parlamentare ha attribuito le proposte del Digital Omnibus on AI alle commissioni per il mercato interno e la protezione dei consumatori (**IMCO**) e per le libertà civili, la giustizia e gli affari interni (**LIBE**), in un assetto di codecisione che riflette la trasversalità degli interessi in gioco.

L'intervento più recente e istituzionalmente significativo del Parlamento europeo è rappresentato dall'adozione di una relazione congiunta del 18 marzo 2026 (*joint report*) da parte delle commissioni IMCO e LIBE. Il documento definisce la posizione negoziale del Parlamento: sulle **scadenze per i sistemi ad alto rischio** il Parlamento si allinea all'orientamento del Consiglio, proponendo l'adozione di date fisse per l'applicazione degli obblighi relativi ai sistemi di IA ad alto rischio - 2 dicembre 2027 per i sistemi dell'Allegato III e 2 agosto 2028 per quelli dell'Allegato I - superando la formula originaria della proposta della Commissione che legava l'applicazione delle norme alla disponibilità degli standard tecnici. L'obiettivo è quello di garantire la certezza del diritto per gli operatori del mercato; Si esprime poi su **divieti mirati,** i quali costituiscono un elemento di aggiunta rispetto alla proposta della Commissione. Il Parlamento propone l'introduzione di un divieto specifico per i sistemi di intelligenza artificiale che generano **contenuti sessuali o intimi** senza il consenso esplicito e informato degli interessati, con condizioni rigorose e specifiche nel testo normativo. Tale misura risponde alle preoccupazioni legate alla proliferazione dei cosiddetti *deepfakes* di carattere non consensuale; il trattamento di **categorie particolari di dati** per la correzione dei *bias* viene riformulato dal Parlamento rispetto alla proposta iniziale.

La relazione congiunta cerca un equilibrio tra l'esigenza di garantire una base giuridica chiara per il trattamento dei dati sensibili nei processi di *de-biasing* e la necessità di assicurare che tale trattamento sia strettamente limitato; la reintroduzione **dell'obbligo di registrazione** costituisce uno dei punti di maggiore distanza rispetto alla proposta della Commissione. Contrariamente all'eliminazione prevista dalla Commissione, il Parlamento propone il ripristino di un sistema di **registrazione semplificata** nella banca dati UE anche per i sistemi di IA che invocano l'esenzione dall'alto rischio ai sensi dell'art. 6, par. 3 dell'AI Act; il supporto alle imprese di **medie dimensioni** viene confermato e rafforzato. La relazione conferma l'estensione delle procedure di documentazione tecnica semplificata alle cc.dd. *small mid-caps*, introducendo al contempo modifiche specifiche al regime delle sanzioni per queste categorie di imprese, con l'obiettivo di garantire proporzionalità nell'applicazione delle norme. Viene inoltre previsto un alleggerimento degli oneri per i sistemi di IA già soggetti a normative settoriali specifiche che garantiscano un livello equivalente di conformità; sul tema della alfabetizzazione, il Parlamento adotta una posizione che cerca di bilanciare le istanze di semplificazione con la necessità di preservare la sostanza dell'obbligo. Viene promosso un assetto in cui i fornitori e i *deployer* di sistemi di IA siano tenuti a sostenere il miglioramento delle competenze del proprio personale, mentre la Commissione e gli Stati membri assumono un ruolo di promozione e incoraggiamento dell'alfabetizzazione informatica nell'intera società. La proposta parlamentare intende preservare un nucleo di obbligo concreto a carico degli operatori, evitando che la trasformazione in puro incentivo istituzionale svuoti la norma di efficacia pratica.

7. Qualche osservazione conclusiva

Le tecnologie dell'intelligenza artificiale, e in generale del settore digitale, hanno generato una rivoluzione socioculturale non indifferente. Non riguardano solo quei cambiamenti socioeconomici che attengono alle abitudini quotidiane degli ultimi anni: basti solo pensare al fatto che ormai la gran parte delle persone affidano le proprie domande (*prompt*) a sistemi di IA generativa: che si tratti di chiedere un parere legale, medico o creare un'immagine.

L'impatto, infatti, ha riguardato anche la cultura e la scienza, probabilmente grazie al concorso di un

importante eco mediatico e di una bolla finanziaria ancora in essere. Se si naviga sul web, o si ricerca in banche dati, si può saggiare la mole di produzione scientifica prodotta, solo negli ultimi quattro anni, dalle due parole "intelligenza artificiale" che John McCarthy coniò, a suo tempo, proprio per la loro capacità attrattiva; nel suo caso, capacità di attrarre finanziamenti nella ricerca. Si spazia, così, da guide pratiche a libri e commentari che analizzano le ultime novità normative la cui applicazione viene poco dopo posticipata, messa in dubbio da interventi intermedi o modificate per adattarsi e inseguire gli ultimi cambiamenti che la tecnica produce. È ormai difficile intercettare una conferenza che non sia centrata su queste tecnologie e un dibattito così endemico su un tema senz'altro rivoluzionario rende difficoltoso discernere e analizzare tutta la letteratura. **È come se** si volesse intercettare le voci intonate durante cori da stadio.

Sicché, in un contesto complesso come quello delle nuove tecnologie, negli ultimi anni, si è assistito a un'imbarazzante ipertrofia normativa nell'ordinamento europeo che ha prodotto una serie di regolamenti nel settore digitale in grado di disorientare qualunque operatore. Buona parte della regolamentazione digitale dell'UE, avente un'efficacia orizzontale, si sovrappone a norme settoriali dettagliate già in vigore in diversi settori, generando duplicazioni e oneri aggiuntivi poco utili, soprattutto là dove i rischi oggetto della regolamentazione digitale sono già affrontati nel quadro normativo di riferimento.

A fronte di un tessuto normativo di questo genere, creato negli anni scorsi (in particolare, dal 2019 al 2024), oggi, la Commissione, sollecitata dai "portatori di interesse", si avvede che il sistema progettato nelle recenti "strategie" deve essere modificato e semplificato. È allora preferibile mutare il nome della strategia. Sebbene la motivazione indicata susciti qualche perplessità[10], l'intento di una semplificazione è sicuramente un indicatore da salutare con favore, anche se l'impianto normativo sembra mantenere una struttura tecnico-burocratica che continua a minacciare il principio della neutralità tecnologica.

Ma ciò che probabilmente desta maggiore perplessità è l'intento espresso nel programma, ad oggi, del tutto irraggiungibile nello scacchiere globale. L'obiettivo di un'UE leader nell'IA, alle condizioni attuali, rimane una evidente utopia. Pur volendo sorvolare sulle differenze di investimenti tra UE e i due principali attori mondiali nel settore, la "sfida" viene principalmente decisa sul campo dei costi dell'energia[11]. Un campo, questo, dove l'UE **è in evidente svantaggio.** Se a questi elementi si aggiunge una normativa europea poco flessibile, non chiara, disordinata e ospite di antinomie, allora il risultato è piuttosto scontato. *Rebus sic stantibus*, l'UE può quindi ambire a rimanere solo una "potenza normativa". L'unica fonte di speranza, minata evidentemente da forze esterne, può essere intercettata in un'iniziativa politica che intervenga sulle infrastrutture digitali come quella sulla "sovranità tecnologica", ma il tempo, si sa, è tiranno.

Il testo definitivo del *Digital Omnibus Act*, che emergerà al termine dei triloghi, perciò, sarà destinato a ridisegnare in modo significativo il quadro normativo digitale europeo per gli anni a venire e inciderà profondamente sulle modalità con cui imprese, pubbliche amministrazioni e cittadini interagiscono con i dati, le piattaforme e i sistemi di intelligenza artificiale negli Stati membri dell'Unione Europea.

10 Come già accennato nel § 1, una delle principali motivazioni è costituita dallo sviluppo della IA generativa. Ciò rende evidente che una impostazione di questo genere porta a "inseguire" gli sviluppi della tecnica, spesso finendo per subirla.

11 Jensen Huang, CEO di Nvidia, durante il AI Summit del Financial Times del 2025, ha dichiarato che, ad oggi, la Cina è destinata a vincere la corsa all'IA, riportando, tra le ragioni della previsione, il fatto che gode di costi energetici inferiori e, in modo un po' sorprendente, di una regolamentazione "minore" rispetto agli Stati Uniti.
Si può aggiungere che un altro fattore importante, a livello competitivo, è rappresentato dall'adozione di modelli open source, consentendo di sfruttare le competenze da parte di diversi sviluppatori e ingegneri nel miglioramento dei codici.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it