CONFINDUSTRIA

Semplificazione in ambito digitale: le priorità dell'industria italiana

Aprile 2026

Position Paper

Sommario

1. Executive Summary

Il presente Position Paper esprime la posizione di Confindustria sulle proposte di Regolamento del Digital Omnibus, con riferimento ai quattro ambiti tematici principali: intelligenza artificiale (all'interno del Digital Omnibus on AI), cybersecurity, protezione dei dati personali e Data Act. Pur condividendo e apprezzando l'impostazione complessiva del pacchetto, orientato alla semplificazione e all'armonizzazione del quadro regolatorio europeo in materia digitale, Confindustria segnala l'esigenza di alcuni interventi mirati per garantire maggiore certezza giuridica, proporzionalità degli adempimenti e piena compatibilità con gli obiettivi di competitività e innovazione dell'industria europea.

In materia di **intelligenza artificiale**, Confindustria apprezza l'iniziativa volta a semplificare l'applicazione dell'AI Act tramite il Digital Omnibus on AI. L'auspicio è che le semplificazioni si traducano in una maggiore certezza giuridica per le imprese, in particolare con riferimento ai principi di necessità, proporzionalità e neutralità tecnologica. Si segnalano come prioritari: il mantenimento del compromesso raggiunto dal Parlamento UE su AI literacy; tempi adeguati per l'entrata in vigore dei nuovi obblighi; un maggiore impegno della Commissione nella redazione di linee guida; l'eliminazione della Sezione A dell'Annex I, con una revisione della formulazione proposta dell'art. 110a relativo al Regolamento macchine, la cui attuale rigidezza rischia di generare sovrapposizioni normative e incertezze applicative.

Sul fronte della **cybersecurity**, la proposta di istituire una piattaforma unica di segnalazione degli incidenti in capo a ENISA è apprezzabile, ma insufficiente senza una piena armonizzazione delle soglie, delle tempistiche e dei modelli di reporting. Si propone l'adozione di una soglia unica armonizzata per gli incidenti significativi, l'allineamento delle tempistiche di segnalazione (72 ore, in coerenza con il GDPR) e l'estensione dell'armonizzazione anche al Cyber Resilience Act. Si segnala inoltre la necessità di armonizzare i processi di audit e le valutazioni di conformità tra Stati membri e di estendere l'esonero da responsabilità per le imprese che segnalano incidenti in buona fede all'intero quadro normativo cyber.

In materia di **protezione dei dati personali**, Confindustria accoglie con favore le modifiche al GDPR proposte dal Digital Omnibus, che intervengono su nodi reali emersi in circa otto anni di applicazione. Tra gli interventi più significativi: la precisazione della nozione di dato personale in chiave soggettiva e contestuale; una definizione espressa di ricerca scientifica che ricomprende anche la ricerca industriale e commerciale; l'individuazione del legittimo interesse quale base giuridica per il trattamento dei dati nello sviluppo e nel funzionamento di sistemi e modelli di IA; una deroga specifica per il trattamento involontario e residuale di categorie particolari di dati; nonché significative semplificazioni in materia di notifica dei data breach, DPIA e obblighi di informativa. Si segnala l'opportunità di affrontare anche il tema del rapporto tra titolare e responsabile del trattamento, oggi non contemplato dalla proposta, e l'esigenza di rivedere i meccanismi di consenso fondati su segnali automatizzati in materia di cookie e tracciamento online.

Infine, con riferimento al **Data Act**, Confindustria condivide il principio della promozione dell'economia dei dati, ma segnala l'esigenza di semplificare l'applicazione delle nuove regole, a partire dalla differenziazione del regime di condivisione tra contesti B2C e B2B, dove il dato costituisce una componente funzionale del macchinario e del processo produttivo. Si propone l'introduzione di un sistema di tracciabilità degli interventi sui dati per calibrare la responsabilità anche in termini di sicurezza, di un modello di accesso graduato e basato sul rischio che sia pienamente coordinato con le normative settoriali, e di misure specifiche per la tutela dei trade secret e dei dati sensibili. Sono inoltre necessarie misure di supporto alle imprese, incluso il sostegno finanziario per gli investimenti in servizi innovativi, nonché una revisione dell'impostazione retroattiva degli obblighi contrattuali e una maggiore chiarezza nelle definizioni normative. È fondamentale che i requisiti di interoperabilità siano definiti tramite standard armonizzati sviluppati dal mercato, con il pieno coinvolgimento dell'industria.

2. Intelligenza artificiale - 2025/0359(COD)

L'intelligenza artificiale ha il potenziale di rilanciare la competitività globale dell'industria europea, se verrà adottata estensivamente dal nostro settore privato. Tuttavia, l'AI Act, anche se condivisibile nei suoi principi, sta già creando incertezze e rallentamenti nell'adozione dell'IA in Europa. In questo contesto, Confindustria apprezza l'iniziativa in corso per semplificare l'applicazione dell'AI Act tramite il **Digital Omnibus on AI**, che ha già migliorato diverse regole di incerta applicazione oggi presenti nell'AI Act.

Gli obiettivi di semplificazione che l'AI Omnibus si è prefissato andrebbero sviluppati soprattutto nella chiave di una maggiore certezza giuridica, riducendo al minimo le ambiguità presenti nell'AI Act e offrendo regole pratiche, coerenti e certe per le imprese europee. Alla luce dei triloghi sul dossier, Confindustria ribadisce l'opportunità di poter avere una regolamentazione dell'IA che combini i suoi obiettivi di protezione dei diritti fondamentali con delle regole che non dissuadano la crescita di un settore dal potenziale trasformativo per le imprese europee.

In materia di **AI literacy e competenze**, il compromesso raggiunto recentemente dal Parlamento europeo è compatibile con gli interessi industriali: il datore di lavoro è tenuto a formare il dipendente nell'utilizzo dei sistemi di intelligenza artificiale, ma non può essere ritenuto responsabile se il dipendente non raggiunge un determinato livello di formazione. La visione è condivisa: le competenze di intelligenza artificiale sono prioritarie per la competitività dell'Europa, ma questa necessità non può diventare una fonte di controversie legali a livello lavorativo. Il rischio, in caso contrario, sarebbe di dissuadere gli investimenti nel settore, aumentare le incertezze giuridiche e compromettere il raggiungimento degli obiettivi di semplificazione che il legislatore europeo si è posto.

Condividiamo inoltre pienamente i riferimenti inseriti nel testo ai principi di **necessità, proporzionalità, certezza del diritto e neutralità tecnologica**, che Confindustria considera essenziali per garantire la certezza giuridica e un quadro regolamentare

efficace. Ci auguriamo che tali principi restino alla base delle discussioni in trilogo e che orientino l'intero dossier verso un equilibrio tra regolazione e sostegno all'innovazione.

Vista la complessità delle norme in via di definizione, Confindustria ritiene fondamentale che il sistema industriale disponga di **tempi adeguati** per adattarsi ai nuovi obblighi di compliance, con particolare riferimento ai sistemi ad alto rischio e agli obblighi legati alla general-purpose AI (GPAI). Le date di entrata in vigore dovrebbero essere chiare e prestabilite, anche nel momento in cui le regole dell'AI Act verranno integrate nella legislazione settoriale. Dove possibile, le date dovrebbero essere anche armonizzate tra provider e deployer, al fine di evitare disallineamenti applicativi che genererebbero ulteriore incertezza nell'industria. Allo stesso tempo, tuttavia, l'entrata in vigore richiede necessariamente la disponibilità di standard armonizzati, e le scadenze prefissate dovrebbero riflettere condizioni tecniche e non politiche. Uno dei modi per venire incontro a tutte queste esigenze sarebbe prevedere una flessibilità nell'applicazione delle regole sull'alto rischio fino al 2028–2029. Questo aiuterebbe a evitare effetti distorsivi, blocchi nelle certificazioni, ritardi e un impoverimento dell'offerta europea.

Per quanto riguarda le **linee guida in ambiti specifici dell'AI Act,** l'impegno della Commissione europea nello stilarle andrebbe maggiormente esplicitato nel testo, al fine di chiarire e dare certezza a principi già oggi presenti e in vigore all'interno del Regolamento. Un caso prioritario per l'industria riguarda l'esenzione per i sistemi di intelligenza artificiale utilizzati esclusivamente per attività di ricerca e sviluppo: una maggiore chiarezza su questo punto contribuirebbe a rimuovere ambiguità interpretative che rischiano di frenare l'innovazione e la sperimentazione in settori strategici.

Confindustria condivide infine pienamente **l'eliminazione della Sezione A dell'Annex I e il trasferimento della regolamentazione citata nella Sezione B**. L'eliminazione della Sezione A permette il rispetto delle regole e dei principi dell'AI Act, evitando al contempo sovrapposizioni normative prive di valore aggiunto e duplicazioni documentali con costi ingiustificati, e riaffermando il primato delle normative settoriali, supportate da competenze tecniche consolidate. È una proposta migliorativa che ricalca pienamente lo spirito del Digital Omnibus, rispettando i principi giuridici alla base ma riducendo gli oneri legali e amministrativi per le imprese.

Detto questo, **la formulazione proposta dell'art. 110a**, che modifica il Regolamento macchine prevedendo sia che la Commissione, mediante atti delegati, possa modificare i requisiti essenziali di sicurezza, sia che alcuni requisiti IA siano considerati come "requisiti essenziali" ai fini del regolamento macchine, **risulta critica** per diversi aspetti e potrebbe avere conseguenze legali indeterminate, causando incertezze applicative, considerando anche l'ormai prossima entrata in vigore del Regolamento macchine.

L'irrigidimento della formula usata può creare, infatti, sovrapposizioni (tra i requisiti previsti dal Regolamento AI e quelli già presenti nel Regolamento macchine) e nuovi obblighi che potrebbero, invece, essere integrati con maggiore flessibilità. Si propone a tale proposito di mantenere il wording già utilizzato nell'AI act che prevede che i requisiti "shall be taken into account".

Si ritiene inoltre fondamentale inserire nello stesso articolo **un obbligo di previa consultazione e coinvolgimento delle parti interessate** prima dell'adozione degli atti

delegati, analogamente a quanto già previsto nel Regolamento Macchine (art. 6 e art. 20) per le procedure di emissione delle specifiche comuni.

3. Cybersecurity - 2025/0360(COD)

L'acquis europeo in materia di cybersecurity oggi è il risultato di un accumulo di norme che, nel corso del tempo, hanno risposto a innovazioni tecnologiche, crisi geopolitiche e diversificazione dei rischi informatici. La stratificazione che si è creata in questo modo rischia di rendere la compliance un esercizio burocratico invece che uno strumento efficace di sicurezza. In questa sezione, dunque, si propongono alcune misure di miglioramento del pacchetto, focalizzandosi sull'armonizzazione degli obblighi per le imprese.

Allineare la segnalazione degli incidenti

La proposta della Commissione europea di stabilire una piattaforma unica di segnalazione degli incidenti è un passo nella giusta direzione, ma perde l'occasione di una piena armonizzazione del quadro normativo. Sebbene infatti sia auspicabile che ENISA possa essere responsabile della raccolta e diffusione delle segnalazioni degli incidenti, l'approccio del pacchetto Omnibus mantiene i diversi obblighi e tempistiche previsti dalle diverse normative, di fatto preservando gli ostacoli affrontati dalle imprese nella compliance.

Per questi motivi, l'iniziativa di semplificazione potrebbe essere più ambiziosa ed efficace. Si propongono dunque:

- Definizione di una soglia unica armonizzata che identifichi in modo univoco gli incidenti da considerarsi significativi ai fini degli obblighi di segnalazione.
- Allineamento delle tempistiche di segnalazione alle scadenze previste dal GDPR (72 ore dalla conoscenza dell'incidente), prevedendo tempi aggiuntivi per la presentazione di segnalazioni complete che consentano alle organizzazioni di condurre analisi approfondite dell'impatto e delle misure correttive implementate.
- Adozione di un modello standardizzato di segnalazione per tutte le tipologie di comunicazioni che includa la descrizione dettagliata dell'incidente, la valutazione dell'impatto, le misure di mitigazione adottate, oltre a sezioni specifiche per i requisiti peculiari di ciascun regolamento.
- Risoluzione dei conflitti normativi settoriali, per esempio tra DORA e il rimanente acquis europeo di cybersecurity, prevedendo esenzioni più ampie per obblighi già coperti a livello di settore, come già disposto, per esempio, nel campo dei dispositivi medici.

Si segnala, infine, che l'adozione di una piattaforma unica di segnalazione per gli incidenti in capo a ENISA rischia di rivelarsi un single point of failure per tutto il sistema di governance della sicurezza informatica. Se non accompagnata da una vera armonizzazione, l'introduzione della piattaforma potrebbe essere controproducente.

Ulteriori spazi di armonizzazione del quadro regolatorio cyber

Il Cyber Resilience Act (CRA) è una norma fortemente significativa per i produttori hardware e software, incidendo sul design dei loro prodotti e servizi. Sembra dunque opportuno che tutte le norme di armonizzazione degli obblighi nel quadro regolatorio di cybersecurity includano anche una revisione del CRA, per uniformare e semplificare il lavoro di compliance che attende le imprese.

Inoltre, l'Unione europea, con i pacchetti Omnibus, ha l'opportunità di armonizzare i processi di audit e valutazione della conformità in ambito cybersicurezza, facilitando il riconoscimento reciproco delle certificazioni tra autorità nazionali.

Attualmente, le imprese che operano in più Stati membri si trovano a dover affrontare procedure di verifica difformi e spesso ripetitive, con conseguenti duplicazioni di costi e tempi che penalizzano particolarmente le PMI e ostacolano il funzionamento del mercato unico digitale. L'adozione di standard comuni per gli audit e il mutuo riconoscimento delle valutazioni effettuate dalle autorità competenti di ciascuno Stato membro ridurrebbe significativamente gli oneri amministrativi, pur garantendo la sicurezza informatica in tutta l'Unione.

Esonero da responsabilità per imprese che segnalano incidenti

L'art. 23 della direttiva NIS 2 specifica che "la sola notifica [di incidente] non espone il soggetto che la effettua a una maggiore responsabilità". Questo principio è imprescindibile per garantire che le imprese possano segnalare gli incidenti senza temere ripercussioni.

Per questo motivo, sembra opportuno che la stessa misura si applichi anche alle notifiche richieste dall'intero quadro regolatorio di sicurezza informatica, prevedendo un esonero completo che protegga le entità segnalanti dalle conseguenze legali derivanti dalle informazioni condivise in buona fede.

4. Protezione dei dati personali - 2025/0360(COD)

Valutazioni di carattere generale

Confindustria ha accolto con favore la scelta della Commissione europea di intervenire, nell'ambito della proposta di Regolamento c.d. Digital Omnibus, sul Regolamento (UE) 2016/679, c.d. GDPR. Si tratta, infatti, di una riforma necessaria per perseguire una più effettiva semplificazione del quadro normativo europeo in materia digitale, rafforzandone al contempo coerenza, certezza applicativa e funzionalità rispetto agli obiettivi di competitività e innovazione.

A circa otto anni dalla sua entrata in operatività, il GDPR ha contribuito a innalzare gli standard di protezione dei dati personali nell'Unione europea e a diffondere nel sistema economico una maggiore attenzione al loro utilizzo corretto e responsabile. Le imprese hanno sostenuto rilevanti sforzi organizzativi, tecnici ed economici per conformarsi alla

normativa, operando in un contesto regolatorio e tecnologico in continua e rapida evoluzione.

L'esperienza applicativa ha, tuttavia, evidenziato criticità significative, riconducibili in particolare alla frammentazione interpretativa, all'onerosità di alcuni adempimenti e a un approccio spesso eccessivamente formalistico. Ne sono derivati margini di incertezza e costi di conformità elevati, che hanno rallentato la capacità delle imprese di innovare, investire e valorizzare pienamente il potenziale dei dati, anche nei processi di trasformazione digitale e nell'adozione di tecnologie *data-driven*.

In questo contesto, il Digital Omnibus interviene su nodi reali emersi nell'implementazione del GDPR. In particolare, la proposta si muove lungo tre direttrici principali: ***i)*** aggiornare e chiarire alcuni aspetti centrali della disciplina in materia di dati personali; ***ii)*** semplificare obblighi particolarmente gravosi; ***ii)*** favorire l'uso dei dati personali per finalità di ricerca e sviluppo di sistemi e modelli di IA.

Per il sistema produttivo italiano **tale impostazione è particolarmente rilevante**. Il tessuto industriale nazionale, caratterizzato da filiere articolate, forte presenza di PMI, crescente integrazione tra manifattura, servizi digitali, ricerca industriale e intelligenza artificiale (IA), richiede un **quadro in materia di protezione dei dati personali che coniughi elevati livelli di protezione, certezza e proporzionalità degli adempimenti e possibilità di utilizzare i dati in modo lecito, responsabile e funzionale allo sviluppo tecnologico**. In quest'ottica, occorre riportare la normativa sulla protezione dei dati personali a una logica maggiormente *risk-based*, favorendo una disciplina più calibrata sulle concrete condizioni del trattamento e riequilibrando il rapporto tra protezione dei diritti e sostenibilità della *compliance*. In tal senso, appare condivisibile l'orientamento richiamato dalla Joint Opinion n. 1/2026 del Comitato europeo per la protezione dei dati (EDPB) e del Garante europeo della protezione dei dati (EDPS), secondo cui la riduzione degli oneri amministrativi deve essere perseguita senza compromettere il livello di protezione dei dati personali e la certezza giuridica per gli operatori.

Il Digital Omnibus cerca di rispondere a questa esigenza: è, quindi, **fondamentale che durante l'*iter* di approvazione ne venga preservata l'impostazione di semplificazione** e che il negoziato europeo consolidi un quadro più aderente alla realtà operativa delle imprese, così da rendere la tutela dei dati pienamente compatibile con una politica industriale europea fondata su innovazione, investimenti e crescita.

Di seguito, alcune considerazioni sulle misure di maggior interesse per le imprese.

Valutazioni di dettaglio

Nozione di dato personale

Tra gli interventi di maggiore rilievo contenuti nel Digital Omnibus vi è la **modifica della definizione di "dato personale"** (art. 4, par. 1, n. 1 del GDPR), che incide su uno dei nodi più problematici emersi nell'applicazione del GDPR. L'attuale ampiezza della nozione ha, infatti, contribuito a ricondurre nel perimetro del GDPR anche informazioni

che, per il soggetto che le tratta, non consentono in concreto l'identificazione della persona a cui si riferiscono.

In linea con quanto stabilito dalla Corte di Giustizia dell'UE[1], la proposta precisa che un'informazione **non può essere qualificata come dato personale in termini assoluti e astratti**, ma che tale qualificazione deve essere condotta tenendo conto del contesto del trattamento e dei mezzi ragionevolmente utilizzabili dal soggetto che detiene l'informazione per identificare l'interessato.

Il tema assume un rilievo specifico con riferimento ai dati pseudonimizzati, rispetto ai quali la proposta valorizza la dimensione soggettiva dell'identificabilità. In questo senso, il fatto che un altro soggetto possa disporre di elementi ulteriori per risalire all'identità dell'interessato non implica, di per sé, che il dato debba essere considerato personale per chiunque lo tratti.

Si tratta, quindi, di un **chiarimento significativo**, che consente di superare letture della nozione di dato personale non sempre coerenti con il rischio concreto del trattamento e che hanno reso più complesso l'utilizzo dei dati in contesti di ricerca e sviluppo.

Ad ogni modo, particolare attenzione dovrà essere riservata al profilo del rischio effettivo di identificazione degli interessati. In questa prospettiva, risulterà fondamentale disporre di criteri interpretativi e applicativi uniformi, anche mediante apposite linee guida dell'EDPB, al fine di assicurare un approccio coerente nella valutazione del rischio di identificazione, nonché di agevolare l'individuazione di misure tecniche e organizzative adeguate a contenerlo.

Ricerca scientifica

Il Digital Omnibus propone una serie di modifiche in materia di ricerca scientifica, volte a precisare il regime applicabile ai trattamenti dei dati personali effettuati in tale ambito e a creare condizioni normative più chiare e favorevoli per la ricerca industriale, lo sviluppo tecnologico e l'innovazione. Nel complesso, le misure sono condivisibili e si auspica vengano confermate durante l'*iter* di approvazione della proposta.

In particolare, si introduce una **definizione espressa di "ricerca scientifica"** (nuovo art. 4, par. 1, n. 38 del GDPR), che ricomprende qualsiasi attività di ricerca idonea sostenere anche l'innovazione, come lo sviluppo tecnologico e la sperimentazione. Al riguardo, si specifica che tali attività devono: ***i)*** contribuire alla conoscenza scientifica esistente ovvero applicare in modo nuovo conoscenze già acquisite; ***ii)*** essere svolte con l'obiettivo di accrescere il patrimonio generale di conoscenze e il benessere della società; ***iii)*** rispettare gli standard etici del pertinente settore di ricerca. Inoltre, si precisa che la ricerca scientifica può avere finalità commerciali.

L'intervento è senz'altro positivo, in quanto riconosce in modo esplicito il ruolo delle imprese nella crescita delle conoscenze e nel benessere della società, rendendo più chiari i confini di liceità dei trattamenti di dati personali effettuati per finalità di ricerca

[1] Sentenza 4 settembre 2025 - causa C-413/235.

scientifica. A tal fine, infatti, ciò che risulta determinante è **l'approccio metodologico e sistematico adottato** e non l'ambito in cui la ricerca o lo sviluppo tecnologico vengono condotti, potendo essere svolti in contesti accademici, ***industriali*** o ***in altri ambienti, comprese le piccole e medie imprese*** (Considerando n. 28 del Digital Omnibus).

Parimenti rilevante è il chiarimento secondo cui il trattamento dei dati personali per finalità di ricerca scientifica può fondarsi, ricorrendone le condizioni (che la ricerca non sia contraria al diritto UE o nazionale e siano rispettate tutte le altre condizioni previste dall'art. 6, par. 1, lett. f) del GDPR, c.d. bilanciamento di interessi), anche sul **legittimo interesse del titolare**, rafforzando così la certezza circa le basi giuridiche utilizzabili in questo ambito (Considerando n. 32 del Digital Omnibus).

Nella medesima direzione, si colloca la modifica del c.d. **principio di limitazione della finalità** (art. 5, par. 1, lett. b) del GDPR), che considera compatibile con le finalità iniziali il trattamento ulteriore per ricerca scientifica, indipendentemente dalle condizioni dell'art. 6, par. 4 del GDPR e, dunque, senza la necessità di verificare preliminarmente la compatibilità del trattamento ulteriore in base al nesso tra le finalità originarie e quelle ulteriori, al contesto in cui i dati sono raccolti, alla natura dei dati, alle conseguenze del trattamento ulteriore trattamento e all'esistenza di garanzie adeguate.

La modifica riduce un passaggio applicativo che, nella prassi, si è spesso tradotto in un fattore di incertezza e in un ostacolo al riutilizzo lecito dei dati per attività di ricerca e innovazione. In quest'ottica, la previsione appare coerente con l'esigenza di favorire una più ampia circolazione e valorizzazione dei dati nei processi di sviluppo tecnologico, senza per questo attenuare le garanzie sostanziali poste dal GDPR, che continuano a trovare applicazione. Inoltre, la modifica consente di riequilibrare il rapporto tra tutela dei diritti e possibilità di impiego secondario dei dati in ambiti che presentano un elevato valore economico, scientifico e industriale.

Infine, viene confermata e meglio precisata la **deroga agli obblighi di informativa** nei casi in cui, per trattamenti effettuati per finalità di ricerca scientifica, la comunicazione all'interessato risulti impossibile, comporti uno sforzo sproporzionato o rischi di rendere impossibile o compromettere seriamente il conseguimento degli obiettivi della ricerca (art. 13, par. 5 del GDPR). Sul punto, il Considerando n. 37 del Digital Omnibus precisa che la fornitura dell'informativa può comportare uno sforzo sproporzionato, in particolare, quando, al momento della raccolta dei dati, il titolare non sapeva, né prevedeva che li avrebbe trattati successivamente per finalità di ricerca scientifica e, quindi, potrebbe non disporre facilmente dei dati di contatto degli interessati. In tali situazioni, il titolare può informare gli interessati in modo indiretto, ad esempio, rendendo pubblicamente disponibili le informazioni, con modalità idonee - da individuare in base al contesto del progetto di ricerca e alle categorie di interessati coinvolti - a raggiungere il maggior numero possibile di interessati. Il chiarimento è importante, in quanto tiene conto dei casi in cui il trattamento per finalità di ricerca scientifica intervenga in una fase successiva rispetto alla raccolta dei dati.

Trattamento dei dati personali nello sviluppo e nel funzionamento di sistemi e modelli di IA

Il Digital Omnibus introduce disposizioni specifiche in materia di intelligenza artificiale, che incidono sul trattamento dei dati personali impiegati per lo sviluppo e il funzionamento di sistemi e modelli di IA, sul regime applicabile ai trattamenti automatizzati e sull'utilizzo, in via residuale, di categorie particolari di dati. Si tratta di misure condivisibili, che si auspica vengano confermate durante l'*iter* di approvazione della proposta, in quanto contribuiscono a delineare un assetto più realistico e funzionale rispetto alle concrete modalità di sviluppo dell'IA senza rinunciare a presidi sostanziali a tutela dei diritti degli interessati.

In primo luogo, la proposta introduce nel GDPR una disposizione specifica sul trattamento nel contesto dello sviluppo e del funzionamento dell'IA (nuovo art. 88-*quater* del GDPR), che individua **il legittimo interesse del titolare** quale base giuridica del trattamento, salvo i casi in cui il diritto dell'Unione o quello nazionale richiedano espressamente il consenso o prevalgano i diritti e le libertà fondamentali dell'interessato.

L'intervento è rilevante, perché interviene su uno dei profili che hanno generato maggiore incertezza applicativa, ossia l'individuazione della base giuridica più idonea per attività di *training*, *testing* e sviluppo di tecnologie emergenti. La norma, peraltro, accompagna questa apertura con **un insieme di garanzie specifiche**, tra cui l'adozione di misure organizzative e tecniche adeguate, l'applicazione del principio di minimizzazione nella selezione delle fonti e nelle fasi di addestramento e test, una trasparenza rafforzata nei confronti degli interessati e il riconoscimento di un diritto incondizionato di opposizione.

Di particolare rilievo è, poi, la nuova **deroga per il trattamento di categorie particolari di dati personali per lo sviluppo e il funzionamento di un sistema o di un modello di IA** (nuovo art. 9, par. 2, lett. k) del GDPR). La misura, muovendo dal presupposto che lo sviluppo dei sistemi e dei modelli di IA comporta la raccolta di grandi quantità di dati, inclusi dati personali e categorie particolari di dati personali, mira a evitare di ostacolare in modo sproporzionato lo sviluppo e il funzionamento dell'IA (Considerando n. 33 del Digital Omnibus).

Ad ogni modo, la nuova deroga opera **solo se il trattamento di categorie particolari di dati è involontario e residuale**. Di regola, infatti, il titolare è tenuto ad adottare adeguate misure tecniche e organizzative per evitare la raccolta e l'utilizzo di dati "sensibili" nei *dataset* impiegati per addestrare, testare o validare sistemi e modelli di IA, nonché a rimuovere quelli che, nonostante tali accorgimenti, vi confluiscano. Solo qualora la rimozione richieda uno sforzo sproporzionato - in particolare, quando comporterebbe la necessità di riprogettare il sistema o il modello di IA -, il trattamento è ammesso a condizione che il titolare protegga efficacemente tali dati e ne impedisca l'uso per generare *output*, nonché la loro divulgazione o il loro accesso da parte di terzi. In tutti gli altri casi, vale a dire quando il trattamento di categorie particolari di dati non è involontario e residuale, ma necessario allo scopo della ricerca, dello sviluppo o del funzionamento del sistema di IA, continua ad applicarsi quanto previsto dall'art. 9, par. 2, lettere da a) a j) del GDPR (Considerando n. 33 del Digital Omnibus).

Infine, positiva anche la **modifica dell'art. 22 del GDPR**, nella parte in cui chiarisce che, ai fini della conclusione o dell'esecuzione di un contratto, una decisione può essere adottata esclusivamente mediante trattamento automatizzato anche quando, in astratto, potrebbe essere assunta da una persona fisica, fermo restando che, tra soluzioni automatizzate ugualmente efficaci, dovrebbe essere privilegiata quella meno invasiva.

Il chiarimento è molto utile, in quanto evita interpretazioni eccessivamente restrittive che rischierebbero di ostacolare, senza adeguata giustificazione, l'impiego di strumenti digitali avanzati e di soluzioni basate su IA nei processi operativi e contrattuali.

Semplificazioni

Il Digital Omnibus introduce misure per semplificare alcuni degli adempimenti che, nell'applicazione del GDPR, hanno generato i maggiori oneri operativi per le imprese.

In particolare, le semplificazioni riguardano:

1. **le attività di notifica dei *data breach*** (art. 33 del GDPR). L'obbligo di notifica dei data breach all'Autorità di controllo (Garante privacy) viene circoscritto alle sole violazioni dei dati personali suscettibili di comportare un rischio elevato per i diritti e le libertà delle persone fisiche, fermo restando l'obbligo di documentare la violazione ex art. 3, par. 5 del GDPR, nonché quello generale di dimostrare la conformità alla disciplina sulla protezione dei dati personali ex art. 5, par. 2 del GDPR (Considerando n. 39 dell'Omnibus Digitale). Inoltre, il termine per la notifica viene esteso da 72 a 96 ore e, ai fini della notifica, si prevede un punto di accesso unico, che lo stesso Digital Omnibus istituisce in capo all'Agenzia dell'Unione europea per la cibersicurezza, c.d. ENISA (nuovo art. 23a della Direttiva NIS 2). È, altresì, prevista la predisposizione, da parte dell'EDPB, di una proposta di modello comune di notifica e di un elenco comune delle circostanze di rischio elevato, che la Commissione potrà poi adottare con atto di esecuzione.

   Gli interventi sono apprezzabili, in quanto consentono di concentrare risorse e attenzione sui casi effettivamente più critici, evitando la proliferazione di notifiche relative a eventi minori che producono un valore limitato sul piano della tutela sostanziale e dell'*enforcement*. L'auspicio è, dunque, che le misure vengano confermate durante l'iter di approvazione della proposta.

   È, altresì, auspicabile che l'istituzione di un punto di accesso unico sia accompagnata non solo da criteri uniformi di valutazione della natura e della gravità degli incidenti oggetto di segnalazione, ma anche da un progressivo allineamento delle relative tempistiche, oggi ancora eterogenee nei diversi quadri normativi. Il GDPR prevede, per i titolari del trattamento, la notifica al Garante entro 72 ore (che la proposta estende a 96 ore) dalla conoscenza della violazione e, ove ricorrano i presupposti, la comunicazione agli interessati senza ingiustificato ritardo; la NIS 2, il DORA e il Cyber Resilience Act, invece, si fondano su modelli di reporting scanditi in più fasi, con segnalazioni iniziali entro 24 ore, aggiornamenti entro 72 ore e relazioni finali entro termini variabili.

In tale prospettiva, merita un approfondimento anche il ruolo del punto di contatto nelle diverse discipline. Sotto il profilo del GDPR, tale funzione non può ritenersi integralmente assorbita dal DPO. Sebbene quest'ultimo, ove obbligatorio, costituisca il presidio interno di riferimento per la *compliance* privacy e l'interlocuzione con l'autorità di controllo, il suo ruolo resta più ampio e distinto rispetto a quello, eminentemente operativo, proprio di un punto unico deputato alla ricezione, al coordinamento e alla trasmissione delle segnalazioni. Ne deriva l'esigenza di chiarire espressamente i rapporti tra le due figure, evitando sovrapposizioni applicative e incertezze organizzative.

Un ulteriore profilo riguarda i gruppi societari transfrontalieri. In tali contesti, la frammentazione degli eventi tra più giurisdizioni e più controllate ha spesso posto criticità nell'individuazione della Autorità di controllo competente. Anche sotto questo aspetto, il punto di accesso unico potrebbe rappresentare uno strumento utile di semplificazione e di maggiore certezza del quadro applicativo;

2. **l'esecuzione della valutazione d'impatto sulla protezione dei dati (DPIA)**. La proposta supera l'attuale assetto fondato su elenchi nazionali, prevedendo che l'EDPB predisponga una proposta di elenco unico europeo dei trattamenti soggetti a DPIA e dei trattamenti esenti, nonché una proposta di modello e metodologia comuni.

   L'intervento è positivo, in quanto mira a rendere la DPIA più omogenea e più utile sul piano sostanziale, considerato che la stessa è anche diretta all'individuazione di misure adeguate al contenimento del rischio. L'esperienza maturata in questi anni ha, infatti, mostrato come la DPIA costituisca, soprattutto per le PMI, uno degli adempimenti più complessi e più esposti a divergenze interpretative tra autorità nazionali, con il rischio di tradursi in un esercizio eccessivamente formale e poco orientato alla gestione sostanziale del rischio. L'auspicio è, dunque, che le misure vengano confermate durante l'*iter* di approvazione della proposta;

3. la **modifica delle circostanze che consentono di derogare all'obbligo di informativa** (art. 13, par. 4 del GDPR). La proposta introduce una nuova deroga all'obbligo di informativa per i trattamenti effettuati nell'ambito di un rapporto chiaro e circoscritto tra l'interessato e il titolare, a condizione che l'attività del titolare non sia d*ata-intensive* (riguardi cioè una ridotta quantità di dati personali e comporti operazioni non complesse), non comporti un rischio elevato e vi siano ragionevoli motivi per ritenere che l'interessato disponga già delle informazioni essenziali sul titolare, sulle finalità e sulla base giuridica del trattamento (es. trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o effettuato sulla base del consenso dell'interessato).

   In tale contesto, potrebbe altresì valutarsi, in specifici settori, l'adozione di modalità di informazione e di gestione del consenso maggiormente semplificate, ferma restando l'esigenza di assicurare in ogni momento l'adeguata conoscenza del trattamento e l'effettiva possibilità di opporsi;

4. **la gestione delle richieste degli interessati, in particolare del diritto di accesso** (art. 12, par. 5, del GDPR). La proposta chiarisce che il titolare può rifiutare la richiesta o chiedere un contributo spese ragionevole non solo nei casi di richieste

manifestamente infondate o ripetitive, ma anche quando emerga un uso abusivo del diritto di accesso per finalità diverse dalla protezione dei dati personali. È, inoltre, previsto un criterio probatorio più realistico per il titolare, che, quanto all'eccessività della richiesta, può fondarsi su ragionevoli motivi.

L'intervento è senz'altro positivo, ma incide solo su un profilo circoscritto degli oneri connessi alla tutela dei diritti degli interessati. Restano, infatti, aperte altre criticità applicative, legate in particolare a una concezione di tali diritti in termini pressoché assoluti, senza un adeguato bilanciamento con i diritti, le libertà e gli obblighi giuridici di altri soggetti, nonché alle modalità di verifica dell'identità del richiedente, che possono tradursi in un aggravio amministrativo sproporzionato per le imprese. Si tratta di aspetti che meritano di essere affrontati più compiutamente nel corso dell'*iter* di approvazione della proposta, al fine di assicurare un esercizio dei diritti più equilibrato e coerente con le concrete condizioni operative dei titolari.

Verifica biometrica dell'identità decentralizzata

Il Digital Omnibus introduce una specifica deroga per il trattamento di dati biometrici ai fini della verifica dell'identità decentralizzata, nei casi in cui il dato biometrico o il mezzo di verifica resti sotto il controllo esclusivo dell'interessato (nuovo art. 9, par. 2, lett. l) del GDPR).

La previsione è condivisibile, in quanto riconosce che, in simili architetture tecnologiche, il rischio per i diritti e le libertà fondamentali risulta significativamente attenuato, poiché il titolare non entra ordinariamente nella piena disponibilità del dato biometrico o vi accede solo in modo limitato e strettamente funzionale al processo di verifica.

La modifica appare coerente con l'evoluzione dei modelli di identità digitale e con l'esigenza di favorire strumenti di autenticazione più sicuri, interoperabili e conformi al principio di minimizzazione. In tale contesto, essa contribuisce a definire un quadro più favorevole allo sviluppo di soluzioni digitali affidabili, senza pregiudicare la protezione dei dati biometrici.

In questo ambito, meriterebbe, altresì, attenzione il tema del possibile rilievo del legittimo interesse del titolare nei trattamenti di dati biometrici effettuati per finalità di identificazione in campo digitale, alla luce del crescente favore dell'ordinamento per procedure di riconoscimento a distanza nella fase precontrattuale, anche ai fini della prevenzione delle frodi e del furto di identità. Si pensi, ad esempio, ai processi di *digital onboarding* nei settori bancario, finanziario e assicurativo. Nel bilanciamento tra i contrapposti interessi, potrebbe, pertanto, attribuirsi adeguato rilievo al grado di affidabilità che il dato biometrico è in grado di offrire ai fini dell'identificazione del cliente, anche in relazione agli obblighi di adeguata verifica previsti dalla normativa antiriciclaggio.

Cookie, tracciamento *online* e coordinamento con la Direttiva ePrivacy

Il Digital Omnibus interviene anche sul rapporto tra il GDPR e la Direttiva 2002/58/CE, c.d. Direttiva ePrivacy, affrontando un profilo che richiede da tempo una revisione più organica e coerente con le esigenze dell'economia digitale.

In particolare, la proposta riorganizza gli obblighi relativi ai *cookie* e al tracciamento *online* e ne trasferisce la disciplina nel GDPR (nuovi artt. 88-*bis* e 88-*ter* del GDPR).

Nel merito, si condivide l'introduzione di regole più semplici per rendere o rifiutare il consenso, nonché la previsione di casi in cui il consenso non è necessario, ad esempio per finalità interne di misurazione dell'utenza o per esigenze di sicurezza del servizio.

Non appare, invece, condivisibile il mantenimento di gestione centralizzata del consenso, affidato a *browser*, sistemi operativi o altri intermediari, poiché Una simile impostazione rischia, inoltre, di generare nuove incertezze sul piano della responsabilità e di accrescere, anziché ridurre, la complessità regolatoria per le imprese.

la scelta di promuovere segnali automatizzati e *machine-readable* di consenso, rifiuto o opposizione, che la proposta collega, in particolare, alle interfacce *online* dei titolari e, per i *browser* non-SME, all'obbligo di mettere a disposizione strumenti tecnici idonei. Sebbene la Commissione europea presenti questa soluzione come leva di semplificazione, essa rischia di allontanare la raccolta del consenso dal contesto concreto del trattamento, con possibili ricadute sulla specificità dell'informazione, sulla ripartizione delle responsabilità e sulla certezza applicativa. Ai sensi del GDPR, infatti, il consenso deve essere informato e specifico rispetto alle concrete finalità del trattamento e la sua raccolta non può essere adeguatamente rimessa a soggetti estranei al rapporto diretto tra titolare e interessato.

In questa prospettiva, si auspica che durante l'iter di approvazione siano mantenute le semplificazioni sui *banner* e sulle modalità di rifiuto del consenso, ma siano rivisti i meccanismi fondati su segnali automatizzati, così da preservare il legame diretto tra titolare, finalità del trattamento e scelta informata dell'interessato.

Il rapporto tra titolare e responsabile del trattamento

Il Digital Omnibus non affronta in modo specifico il tema dei rapporti tra titolari e responsabili del trattamento (artt. 28 e ss. GDPR).

Si tratta, tuttavia, di un profilo di particolare rilievo, soprattutto per le PMI, che spesso non dispongono né della forza contrattuale, né del *know-how* tecnologico che il GDPR, almeno in parte, presuppone in capo al titolare ai fini delle istruzioni da impartire al fornitore, dell'individuazione delle misure di sicurezza e dell'esercizio di effettivi poteri di verifica e controllo, *audit* inclusi. A ciò si aggiunge che la filiera dei fornitori, specie nei contesti digitali più evoluti, risulta oggi ben più articolata e complessa rispetto allo schema lineare titolare-responsabile-sub-responsabile delineato dal GDPR; complessità di cui non sembra tenere pienamente conto neppure l'attuale impianto delle clausole tipo per i trasferimenti transfrontalieri di dati.

Analogamente, la proposta non pare soffermarsi in modo adeguato sull'impatto dei servizi di *cloud computing*, nonostante la centralità ormai assunta da tali modelli anche alla luce delle politiche europee e nazionali volte a promuoverne l'adozione. In questo campo, il tradizionale assetto dei ruoli e delle responsabilità appare, in diversi casi, solo parzialmente idoneo a riflettere l'effettiva distribuzione del potere contrattuale e del controllo tecnico lungo la catena dei fornitori.

In tale prospettiva, potrebbe risultare opportuna una riflessione del legislatore europeo su possibili interventi di semplificazione e di riequilibrio, idonei a garantire una maggiore tutela alle imprese titolari del trattamento, e in particolare alle PMI, che frequentemente si trovano a sopportare obblighi e responsabilità non sempre coerenti con la loro concreta posizione nei rapporti con i fornitori, specie in ambito IT.

5. Dati - 2025/0360(COD)

Confindustria ha condiviso fin dall'inizio il principio alla base del Data Act, volto a promuovere l'economia dei dati, a riconoscerne il valore economico lungo l'intera catena del valore e, soprattutto, a creare nuove opportunità di business capaci di sostenere la crescita industriale e il posizionamento strategico del Paese negli investimenti innovativi.

Tale obiettivo, tuttavia, è stato perseguito attraverso la costruzione di un quadro normativo articolato e complesso, la cui attuazione comporta per le imprese rilevanti oneri di compliance, sia sotto il profilo organizzativo sia sotto quello tecnico. Il Data Act richiede infatti un'analisi continua e granulare di ogni tipologia di dato generato dai prodotti, al fine di definirne modalità di accesso conformi. Si tratta di un obbligo permanente, che si estende a tutte le varianti di prodotto, alle versioni firmware e ai diversi contesti operativi, con un impatto significativo in termini di risorse tecniche e organizzative.

A ciò si è aggiunto un ulteriore rallentamento nella corretta attuazione del Regolamento, dovuto sia alla mancata tempestiva pubblicazione dei termini e delle condizioni contrattuali per la condivisione dei dati, sia, a livello nazionale, alla mancata individuazione dell'autorità competente.

Per queste ragioni, pur ritenendo che il Digital Omnibus si muova nella giusta direzione, in quanto orientato alla semplificazione e all'armonizzazione del quadro regolatorio, occorrono adeguamenti mirati per evitare rischi sotto il profilo della sicurezza, dell'innovazione e della responsabilità.

In particolare, il principio di condivisione e accessibilità dei dati assume una portata particolarmente incisiva nei rapporti B2B, dove il dato non rappresenta un semplice sottoprodotto del bene connesso, ma costituisce una componente funzionale del macchinario e del processo produttivo. Per questo motivo, applicare ai rapporti tra imprese la stessa logica di condivisione prevista per il B2C rischia di compromettere i requisiti di sicurezza e conformità, nonché la protezione dei beni intangibili.

Per tale ragione, si dovrebbero introdurre **due regimi differenziati**: uno più semplice, orientato al consumatore, e un altro più avanzato per il contesto **B2B**, corredato da misure specifiche idonee ad assicurare la coerenza con le molteplici normative, generali

e settoriali, a presidio della sicurezza e della conformità dei prodotti, quali, ad esempio, il Regolamento Macchine e il Cyber Resilience Act.

Interventi esterni sui dati, infatti, possono determinare "modifiche sostanziali", con ricadute sulla conformità e sulla **sicurezza del prodotto,** oltre a generare difficoltà nell'accertamento delle responsabilità e un ingiustificato trasferimento dei rischi sul produttore, pur in assenza di un suo controllo diretto sul processo.

In questa prospettiva, dovrebbe essere introdotto un sistema di **tracciabilità degli interventi sui dati**, che ne assicuri il controllo e consenta l'individuazione delle **responsabilità in caso di violazioni.** A tal fine, si potrebbero prevedere sia registri delle modifiche digitali sia l'impiego di strumenti firmati digitalmente, così da graduare correttamente la responsabilità in caso di operazioni non conformi.

L'esigenza di superare un approccio normativo puramente orizzontale, che rischierebbe di penalizzare prodotti e servizi particolarmente complessi, risulta evidente in diversi ambiti. Da un lato, per i **settori critici** è indispensabile prevedere un regime dedicato ai sistemi di controllo e ai parametri *safety-critical,* ad esempio vincolando gli accessi all'uso esclusivo di strumenti certificati, tracciati e auditabili. Dall'altro, si rende necessaria un'ulteriore valutazione specifica per quei **settori che sono già disciplinati da normative di settore**, in particolar modo per ciò che concerne il delicato trattamento dei **dati sensibili.**

Anche sul fronte della tutela dei **trade secret,** pur essendo positivo il rafforzamento delle garanzie nei casi di rischio di acquisizione illecita da parte di Paesi terzi, permane una rilevante difficoltà applicativa. I dati sono spesso generati in modo continuo e si presentano in insiemi eterogenei, all'interno dei quali risulta, di fatto, impossibile distinguere con certezza i dati coperti da segreto commerciale da quelli liberamente condivisibili. Per questa ragione, le imprese sono spesso costrette a trattare integralmente i dataset misti come riservati, con un conseguente aggravio nella gestione delle misure necessarie a tutelarne la riservatezza. L'onere amministrativo e tecnico che ne deriva è estremamente elevato e assorbe risorse ingegneristiche già limitate.

Va inoltre ricordato che un elevato rischio di *disclosure* accidentale del *know-how* ne determinerebbe la perdita di valore economico e, quindi, del vantaggio competitivo dell'impresa che ha investito nella generazione e nella protezione di tali asset.

In questa direzione, sarebbe opportuno introdurre u**n modello di accesso graduato e basato sul rischio,** capace di regolare la disponibilità delle informazioni, bilanciando adeguatamente i diritti dell'utilizzatore, la tutela della proprietà intellettuale e dei dati sensibili, la sicurezza del prodotto e la sostenibilità economica.

Nell'immediato, è necessario accompagnare le imprese con **misure di supporto** volte a semplificare l'adeguamento agli obblighi di accessibilità by design, di adozione dei requisiti di sicurezza e conformità, nonché di gestione e tutela dei trade secret e dei dati sensibili, ad esempio attraverso linee guida, migliori pratiche attuabili e supporto economico e gestionale per l'adozione di strumenti tecnologici innovativi.

Tra gli oneri applicativi merita poi particolare attenzione il tema della **retroattività**. Il Data Act introduce infatti obblighi suscettibili di incidere anche su contratti già in essere,

alterando ex post gli equilibri negoziali raggiunti tra le parti e imponendo alle imprese di riaprire rapporti contrattuali già conclusi. Sarebbe pertanto opportuno cogliere l'occasione del Digital Omnibus per rivedere tale impostazione e assicurare maggiore certezza e coerenza applicativa.

Infine, occorre evidenziare che molte difficoltà derivano anche dall'ampiezza e dalla **genericità di alcune disposizioni e definizioni,** tra cui quelle di "servizio di elaborazione dei dati", "servizio connesso" e "servizio di trattamento dei dati", che si prestano a interpretazioni più o meno estensive, a detrimento della certezza del quadro normativo e con il rischio di alimentare il contenzioso.

È inoltre condivisibile la conferma del divieto di imporre obblighi di residenza nazionale dei dati introdotto dal Free Flow of Non-Personal Data Regulation nell'ottica di rafforzare l'economia europea dei dati e, nel lungo periodo, la sovranità tecnologica dell'Unione. Nel contesto del mercato unico, eventuali requisiti di localizzazione nazionali sarebbero infatti in contrasto con il principio del "one Europe, one market", ribadito anche dal Consiglio europeo.

Con riferimento alle misure di **switching nei servizi cloud**, sono condivisibili gli interventi volti a favorire gli investimenti delle PMI e delle imprese a media capitalizzazione nei servizi di fornitura cloud.

È fondamentale che l'eventuale definizione di requisiti comuni in tema di interoperabilità avvenga anzitutto tramite standard armonizzati predisposti dagli organismi di standardizzazione riconosciuti a livello europeo e internazionale, quali ISO, CEN, ETSI e IETF, con il pieno coinvolgimento dell'industria, anziché attraverso *common specifications* introdotte per via regolatoria. Considerata la rapida evoluzione dei servizi digitali, soltanto un modello basato su standard sviluppati dal mercato può assicurare un quadro realmente orientato al futuro, in grado di promuovere l'interoperabilità senza ostacolare l'innovazione tecnologica.

In conclusione, è opportuno cogliere l'occasione del Digital Omnibus per introdurre **misure specifiche per il data sharing B2B**, che consentano una più efficace gestione del rischio e una maggiore coerenza con la normativa sulla sicurezza dei prodotti e le normative specifiche di settore. Per favorire lo sviluppo e la crescita della economia dei dati, è importante adottare misure e **strumenti anche a livello finanziario**, a supporto degli **investimenti in servizi innovativi e tecnologici avanzati** che il Data Act rende possibili quali, per esempio: la creazione di nuovi servizi a valore aggiunto; nuovi modelli di business cloud-friendly; riprogettazione dei prodotti e dei modelli di business per consentire il data sharing by design; assistenza personalizzata nei servizi cloud e data sharing; consulenza per la compliance contrattuale, formazione e *awareness*.

Un **sistema strutturato di supporto alle imprese** e **quadro europeo più maturo** consentirebbe di cogliere le molteplici opportunità legate all'economia dei dati, di liberare il loro valore economico e assicurare lo sviluppo e la resilienza del sistema innovativo europeo. Solo attraverso un'effettiva **semplificazione attuativa** sarà possibile favorire la diffusione della cultura dell'economia dei dati e la corretta valorizzazione economica, cogliendo appieno il potenziale di sviluppo di questo mercato a livello europeo.