IBM Italia S.p.A.
Circonvallazione Idroscalo
20054 Segrate

MEMORIA SCRITTA

DI IBM ITALIA

Camera dei deputati – Commissione XIV (Politiche dell'Unione Europea)

Proposta di regolamento Del Parlamento europeo e del Consiglio che istituisce un quadro di misure per rafforzare l'ecosistema europeo del Cloud e dell'IA (Cloud and AI Development Act - CADA)

14 ottobre 2026

Indice

1. **Premessa** 2
2. **Una sovranità digitale fondata su governance e libertà di scelta** 3
3. **La definizione di subfornitore** 4
4. **Chiarezza sul perimetro del servizio sottoposto ad audit** 5
5. **Metadati, telemetria e attività di supporto** 5
6. **I criteri relativi al controllo di Paesi terzi** 6
7. **Supply chain software e open source** 7
8. **Sanzioni ed embarghi di Paesi terzi** 8
9. **Principi per un quadro normativo efficace** 8
10. **Considerazioni finali** 9

IBM ITALIA S.p.A.
Società con unico azionista
Soggetta all'attività di direzione e coordinamento di
International Business Machines Corporation
Cap. Int. Versato Euro 247.656.998,20
Cod. Fisc. e Reg. Imprese di:
Milano Monza Brianza Lodi N. 01442240030
Partita IVA 10914660153
Sede legale: Circonvallazione Idroscalo
20054 Segrate (MI)

1. **Premessa**

IBM è una delle principali aziende tecnologiche globali, presente in oltre 170 Paesi e attiva in Italia da oltre un secolo. Operando nel mercato business-to-business, collaboriamo con imprese e pubbliche amministrazioni per accompagnarne i percorsi di innovazione e trasformazione digitale attraverso tecnologie quali cloud ibrido, intelligenza artificiale, cybersecurity e gestione dei dati.

L'esperienza maturata nella progettazione, nello sviluppo e nell'erogazione di queste tecnologie ci ha portato a definire alcuni principi che riteniamo essenziali per favorire un'innovazione responsabile, affidabile e sostenibile.

Anzitutto, i dati appartengono ai clienti, che devono mantenerne il pieno controllo, la titolarità e la capacità di scegliere come utilizzarli. In secondo luogo, i sistemi di intelligenza artificiale devono essere trasparenti, spiegabili e verificabili, affinché sia possibile comprenderne il funzionamento, valutarne gli esiti e garantirne un utilizzo responsabile. Riteniamo inoltre che l'intelligenza artificiale debba essere sviluppata e impiegata come strumento di supporto alle persone, valorizzandone competenze e capacità decisionali. La responsabilità finale delle decisioni deve rimanere in capo agli esseri umani.

Un ulteriore elemento che consideriamo fondamentale è l'apertura degli ecosistemi tecnologici. IBM sostiene da tempo modelli basati su standard aperti e open source, che favoriscono interoperabilità, trasparenza, innovazione diffusa e riduzione delle dipendenze tecnologiche. In un contesto caratterizzato da crescente complessità, la possibilità di integrare tecnologie diverse, garantire portabilità dei dati e delle applicazioni e preservare la libertà di scelta delle organizzazioni rappresenta un fattore strategico per la competitività, la resilienza e la sovranità digitale europea.

Questi principi si riflettono anche nella nostra strategia di cloud ibrido, che consente a organizzazioni pubbliche e private di scegliere dove collocare dati e applicazioni sulla base di requisiti di sicurezza, resilienza, conformità normativa e sovranità del dato, evitando vincoli tecnologici e favorendo la massima interoperabilità tra ambienti differenti.

Alla luce di tali principi, IBM accoglie favorevolmente gli obiettivi del *Cloud and AI Development Act,* volti a rafforzare l'ecosistema europeo del cloud e dell'intelligenza artificiale, ampliare la capacità di calcolo disponibile nell'Unione, attrarre investimenti e migliorare la resilienza dei servizi digitali. Riteniamo che il conseguimento di tali obiettivi richieda un quadro normativo che preservi un mercato unico aperto e competitivo, garantisca certezza giuridica e consenta agli operatori di competere sulla base della capacità di soddisfare requisiti chiaramente definiti in materia di sicurezza, resilienza e sostenibilità.

Pur condividendo pienamente le finalità del provvedimento, riteniamo che alcuni aspetti del capitolo relativo all'autonomia e, in particolare, dell'Allegato II dedicato ai requisiti di sovranità per i servizi cloud, possano beneficiare di ulteriori chiarimenti. Una maggiore chiarezza normativa contribuirebbe a rafforzare la certezza del diritto, sostenere gli investimenti nelle infrastrutture digitali europee e garantire una migliore coerenza tra gli strumenti individuati e gli obiettivi perseguiti dal legislatore.

Nella formulazione attuale, alcune disposizioni dell'Allegato II possono infatti determinare ambiguità interpretative e incertezza applicativa per gli operatori che erogano servizi attraverso infrastrutture, catene tecnologiche e competenze distribuite a livello internazionale. Un chiarimento di tali disposizioni permetterebbe di assicurare maggiore prevedibilità del quadro regolatorio e di sostenere gli investimenti nelle capacità digitali europee, in coerenza con gli obiettivi dichiarati del CADA. In questa prospettiva, la presente memoria propone un approccio fondato su alcuni principi guida: centralità del controllo dei dati da parte dei clienti, sovranità operativa dimostrabile e verificabile, sicurezza e resilienza dei servizi, proporzionalità delle misure, interoperabilità e apertura degli ecosistemi tecnologici, promozione dell'innovazione e degli investimenti.

2. **Una sovranità digitale fondata su governance e libertà di scelta**

A giudizio di IBM, la sovranità digitale europea dovrebbe essere definita innanzitutto come la capacità effettiva di organizzazioni pubbliche e private di mantenere il controllo sui propri dati, sulle proprie applicazioni e sui propri processi critici, preservando al tempo stesso la libertà di scegliere le tecnologie e i fornitori più idonei alle proprie esigenze. In questa prospettiva, la sovranità non coincide con la nazionalità del fornitore o con l'origine geografica della tecnologia, bensì con la concreta possibilità per il cliente di esercitare controllo, autonomia decisionale e capacità di governo dei propri asset digitali.

Un elemento essenziale di questa visione è la prevenzione di situazioni di lock-in tecnologico, che possono limitare la concorrenza, ridurre la flessibilità operativa, aumentare i costi di transizione e ostacolare l'innovazione. La sovranità digitale si rafforza quando le organizzazioni hanno la possibilità di migrare dati e applicazioni, adottare strategie multi-cloud e hybrid cloud, integrare soluzioni sviluppate da soggetti diversi e modificare nel tempo le proprie scelte tecnologiche senza vincoli sproporzionati.

Per questa ragione, interoperabilità, portabilità, reversibilità delle applicazioni e dei dati e utilizzo di standard aperti non rappresentano soltanto requisiti tecnici, ma costituiscono strumenti fondamentali per garantire autonomia strategica, resilienza e libertà di scelta. L'open source e gli ecosistemi aperti contribuiscono inoltre a favorire trasparenza, innovazione e concorrenza, rafforzando la capacità delle organizzazioni di mantenere il controllo sulle proprie infrastrutture digitali.

Un approccio fondato prevalentemente su criteri geografici rischierebbe invece di ridurre la concorrenza e la capacità di innovazione senza garantire automaticamente maggiori livelli di sicurezza o autonomia operativa. Al contrario, la sovranità dovrebbe essere valutata sulla base di elementi oggettivi e verificabili, quali il controllo dei dati, la gestione degli accessi privilegiati, la resilienza operativa, la continuità dei servizi, la portabilità delle applicazioni e dei carichi di lavoro e l'assenza di vincoli che impediscano alle organizzazioni di modificare nel tempo le proprie scelte tecnologiche.

In tale prospettiva, anche i criteri previsti dall'Allegato II dovrebbero misurare la sovranità attraverso risultati operativi dimostrabili e garanzie tecniche, giuridiche e organizzative sottoponibili ad audit. La struttura proprietaria, la sede del fornitore o la provenienza geografica delle singole

componenti tecnologiche non assicurano, considerate isolatamente, il controllo effettivo del servizio e non dovrebbero pertanto sostituirsi a una valutazione sostanziale delle misure adottate.

In questo contesto, risultano particolarmente importanti interoperabilità, portabilità, reversibilità delle soluzioni e possibilità di adottare architetture multi-cloud e hybrid cloud, che consentono alle organizzazioni di evitare situazioni di dipendenza tecnologica e rafforzare concretamente il proprio livello di autonomia. La sovranità digitale europea dovrebbe pertanto essere misurata sulla capacità effettiva di garantire controllo, sicurezza, resilienza e libertà di scelta, assicurando alle organizzazioni la possibilità di utilizzare, integrare e sostituire tecnologie differenti all'interno di un ecosistema aperto e competitivo.

3. **La definizione di subfornitore**

La definizione di subfornitore rappresenta un elemento essenziale per assicurare certezza giuridica e proporzionalità nell'applicazione della normativa. È opportuno che tale definizione sia limitata ai soggetti direttamente coinvolti nella fornitura e nell'erogazione del servizio cloud oggetto di audit.

Un'estensione eccessivamente ampia del concetto di subfornitore rischierebbe infatti di ricomprendere soggetti che appartengono all'ecosistema tecnologico complessivo, ma che non rivestono alcuna responsabilità diretta rispetto all'erogazione del servizio. Ciò potrebbe generare obblighi difficilmente applicabili e verificabili, senza produrre benefici concreti in termini di sicurezza, resilienza o sovranità.

In particolare, appare opportuno chiarire, nell’ambito dell’Allegato II, il significato del riferimento al “contributo alla fornitura e all’erogazione” del servizio cloud, affinché gli obblighi siano limitati ai soggetti direttamente coinvolti nell’erogazione del servizio sottoposto ad audit.
In assenza di tale chiarimento, il perimetro potrebbe estendersi a fornitori a monte della catena del valore, sviluppatori di componenti software o altri soggetti dell’ecosistema tecnologico che non esercitano un controllo operativo diretto sul servizio oggetto della valutazione. Una simile interpretazione rischierebbe di introdurre obblighi sproporzionati e difficilmente verificabili, senza apportare benefici concreti agli obiettivi di sovranità, sicurezza e resilienza perseguiti dal regolamento.

Per tali ragioni, appare opportuno adottare una definizione chiara, circoscritta e operativa, che consenta di individuare con precisione le responsabilità effettivamente rilevanti ai fini della valutazione. La definizione dovrebbe quindi comprendere esclusivamente i soggetti direttamente responsabili della fornitura e dell’erogazione del servizio cloud sottoposto ad audit, senza estendersi al più ampio ecosistema tecnologico o ai fornitori a monte privi di responsabilità dirette sulla prestazione del servizio

4. **Chiarezza sul perimetro del servizio sottoposto ad audit**

Un ulteriore elemento di attenzione riguarda la definizione del perimetro del servizio cloud sottoposto a valutazione. Per garantire una corretta applicazione della normativa è necessario chiarire il rapporto tra il servizio oggetto dell'audit e le diverse componenti tecnologiche che ne consentono il funzionamento, comprese piattaforme, sistemi operativi, componenti software, componenti open source e infrastrutture di supporto.

A tal fine, sarebbe utile esplicitare il rapporto tra il livello di servizio oggetto di audit e le componenti tecnologiche sottostanti, distinguendo chiaramente tra servizio, piattaforma, sistema operativo, software, componenti open source e infrastrutture di supporto. Tale chiarezza risulta essenziale per garantire un'applicazione uniforme e prevedibile dei requisiti previsti dall'Allegato II.

Appare inoltre opportuno evitare che requisiti applicabili a un determinato livello del servizio comportino, indirettamente, l'estensione degli obblighi a componenti hardware o infrastrutturali che non rientrano nel perimetro della valutazione. Una delimitazione chiara consentirebbe agli operatori e agli organismi di audit di applicare i requisiti in modo coerente, uniforme e prevedibile.

Risulta, in particolare, necessario assicurare una piena coerenza tra l'Allegato II e l'Allegato III. Qualora l'hardware sia espressamente escluso dal perimetro dell'Allegato II, gli obblighi relativi alla supply chain software non dovrebbero reintrodurre indirettamente requisiti riferiti a hardware, firmware, BIOS, dipendenze tra software e hardware o infrastrutture di supporto.

Le evidenze richieste con riferimento a tali componenti dovrebbero essere limitate a quanto strettamente necessario per valutare la sicurezza, la resilienza e il controllo operativo del servizio cloud sottoposto ad audit. Ciò permetterebbe di evitare un'estensione indiretta dei requisiti UAL[1] oltre il perimetro definito dal regolamento.

5. **Metadati, telemetria e attività di supporto**

Le disposizioni relative alla localizzazione di metadati e telemetria meritano particolare attenzione. È infatti opportuno distinguere chiaramente tra i contenuti e i dati del cliente, che richiedono il massimo livello di protezione e controllo, e le informazioni tecniche utilizzate per finalità operative, di monitoraggio, manutenzione e sicurezza.

In particolare, il trattamento di metadati e telemetria previsto nei livelli UAL1 e UAL2 merita un riesame volto ad assicurare che gli eventuali requisiti di localizzazione siano proporzionati al rischio e compatibili con il funzionamento delle moderne infrastrutture cloud. L'applicazione indistinta di obblighi di localizzazione a entrambe le categorie potrebbe risultare eccessivamente

[1] **UAL** sta per ***Union Assurance Levels*** (livelli di garanzia dell'Unione). Sono i quattro livelli di sovranità che il CADA prevede per i servizi cloud. Le PA li useranno negli appalti per classificare i fornitori. I criteri di ciascun livello sono nell'**Allegato II**. I livelli sono cumulativi: chi ottiene un livello soddisfa anche quelli inferiori.

ampia rispetto agli obiettivi perseguiti, considerata la diversa natura e funzione delle informazioni coinvolte.

Appare pertanto necessario distinguere tra i contenuti e i dati dei clienti, da un lato, e i dati operativi utilizzati per finalità di sicurezza, manutenzione, monitoraggio e risposta agli incidenti, dall'altro. L'accesso controllato ai dati operativi, assistito da adeguate garanzie, non determina necessariamente un rischio per la sovranità o per il controllo esercitato dal cliente sui propri dati.Le moderne infrastrutture cloud si fondano sulla capacità di identificare tempestivamente minacce informatiche, vulnerabilità e anomalie operative. In molti casi ciò richiede l'accesso a competenze altamente specializzate e a team di risposta distribuiti a livello globale. Restrizioni eccessivamente rigide sulla gestione di metadati, telemetria e attività di supporto potrebbero rallentare la capacità di prevenire e gestire incidenti informatici, con effetti potenzialmente negativi sulla sicurezza e sulla resilienza dei servizi.

Particolare attenzione merita la previsione secondo cui, dal livello UAL2, le attività di supporto debbano essere avviate ed eseguite esclusivamente all'interno dell'Unione. In caso di cyberattacchi, vulnerabilità critiche o gravi interruzioni dei servizi, l'accesso tempestivo a team specialistici globali può essere essenziale per assicurare una risposta efficace e ripristinare rapidamente la piena operatività.
Una restrizione geografica assoluta potrebbe quindi rallentare la risposta agli incidenti e, come conseguenza non intenzionale, ridurre la sicurezza e la resilienza dei servizi cloud erogati nell'Unione. Il quadro dovrebbe preservare la possibilità di ricorrere alle migliori competenze disponibili, prevedendo al tempo stesso garanzie adeguate per la protezione dei dati dei clienti, la gestione degli accessi privilegiati e la tracciabilità degli interventi.

Un approccio basato sul rischio, accompagnato da adeguate misure di controllo, tracciabilità e protezione dei dati, consentirebbe di raggiungere un equilibrio più efficace tra esigenze di sovranità, sicurezza e continuità operativa. In tale prospettiva, appare opportuno riconsiderare l'inclusione generalizzata di metadati e telemetria in UAL1 e valutarne attentamente la proporzionalità nell'ambito di UAL2.

6. **I criteri relativi al controllo di Paesi terzi**

I requisiti relativi al controllo di Paesi terzi dovrebbero concentrarsi principalmente sui risultati effettivamente conseguiti in termini di autonomia operativa e protezione degli interessi europei.

Sotto questo profilo, IBM valuta positivamente l'impostazione prevista per UAL2 nella misura in cui essa appare orientata a verificare risultati operativi e misure di controllo effettive, piuttosto che fare affidamento esclusivamente sulla struttura proprietaria del fornitore. Tale impostazione può costituire una base concretamente applicabile per affrontare le esigenze di sovranità attraverso la valutazione del controllo effettivo sul servizio e sui dati.

A tal fine, appare utile definire con maggiore precisione alcuni concetti fondamentali, affinché gli operatori possano comprendere con chiarezza quali misure siano richieste per dimostrare la conformità. L'obiettivo dovrebbe essere quello di verificare l'effettiva capacità di un'organizzazione di mantenere il controllo sui dati, sugli accessi privilegiati, sulle operazioni critiche e sulla continuità del servizio.

In particolare, i concetti di “prevented”, “control” e “necessary measures” richiedono ulteriori precisazioni. In assenza di definizioni puntuali, permane incertezza sul livello di separazione e sulle misure tecniche, organizzative e giuridiche necessarie per dimostrare la conformità ai requisiti di UAL2 e UAL3.

Una valutazione fondata su evidenze tecniche e organizzative verificabili risulterebbe maggiormente coerente con gli obiettivi di sovranità rispetto a criteri basati esclusivamente sull'assetto proprietario, sulla nazionalità degli azionisti o sull'origine geografica dell'operatore.

In particolare, UAL3 dovrebbe fondarsi su una sovranità operativa dimostrabile e non sulla sola struttura proprietaria del provider. L’accesso a tale livello dovrebbe dipendere da garanzie oggettive e sottoponibili ad audit, capaci di dimostrare il controllo indipendente sui dati dei clienti, sugli accessi privilegiati, sulla continuità del servizio e sui processi decisionali operativi.
In tale contesto, appare opportuno valutare attentamente l’interazione tra l’articolo 18 e i criteri previsti per UAL3, affinché le disposizioni non producano involontariamente restrizioni di fatto all’accesso al mercato per operatori con sede al di fuori dell’Unione, anche quando questi ultimi siano in grado di dimostrare una solida indipendenza operativa dei servizi erogati nell’Unione europea.

I criteri relativi al controllo di Paesi terzi dovrebbero quindi basarsi sul controllo operativo trasparente e dimostrabile del servizio sottoposto ad audit. La struttura proprietaria o la nazionalità del personale non dovrebbero costituire elementi determinanti quando non contribuiscano direttamente e in modo verificabile al conseguimento degli obiettivi di sovranità.

7. **Supply chain software e open source**

Il software moderno è sviluppato attraverso ecosistemi complessi e altamente interconnessi. In tale contesto, gli obblighi relativi alla supply chain software dovrebbero rimanere proporzionati e concentrarsi sulla sicurezza e sulla resilienza del servizio erogato.

Con specifico riferimento al criterio I.2 applicabile a UAL2 e UAL3, appare opportuno mantenere un approccio basato sul rischio e sulla proporzionalità. I fornitori di servizi cloud non dovrebbero essere chiamati ad assumere la responsabilità dell’audit o del controllo diretto di componenti software sviluppate, mantenute o governate da soggetti terzi indipendenti, sui quali non dispongono di effettivi poteri di direzione o intervento.

L'open source costituisce oggi una componente fondamentale dell'innovazione digitale e rappresenta un importante fattore di interoperabilità, trasparenza e autonomia tecnologica. Un quadro normativo efficace dovrebbe riconoscere il contributo che tali modelli offrono allo sviluppo di ecosistemi aperti e competitivi.

Ulteriori chiarimenti risultano auspicabili con riferimento a concetti quali “dependencies”, “source-code audits” e “migration plans”. Tali concetti, se non adeguatamente circoscritti, rischiano di risultare difficilmente applicabili in modo uniforme all’interno di ecosistemi digitali complessi, caratterizzati da un elevato numero di dipendenze e da una diffusa presenza di componenti open source sviluppate e governate da comunità o soggetti indipendenti.

Allo stesso tempo, appare opportuno evitare di attribuire ai provider responsabilità che eccedano la loro effettiva capacità di controllo sulle componenti sviluppate e governate da soggetti in-

dipendenti. L'attenzione dovrebbe concentrarsi sulla capacità di identificare, gestire e mitigare i rischi lungo la supply chain, piuttosto che sull'origine geografica delle singole componenti software.

I requisiti di UAL2 e UAL3 dovrebbero pertanto concentrarsi sulla sicurezza, sulla resilienza e sull'integrità del servizio cloud sottoposto ad audit, nonché sull'efficacia dei processi adottati per gestire vulnerabilità e dipendenze. L'origine geografica delle singole componenti software non dovrebbe essere considerata, di per sé, un indicatore della sicurezza o della sovranità del servizio.

8. **Sanzioni ed embarghi di Paesi terzi**

Anche le disposizioni relative ai regimi di sanzioni ed embarghi richiedono un elevato livello di chiarezza e prevedibilità. I requisiti dovrebbero consentire agli operatori e agli organismi di controllo di comprendere con precisione quali evidenze siano necessarie per dimostrare la conformità e quali elementi debbano essere considerati nella valutazione.

Con specifico riferimento al criterio G.4, applicabile ai livelli UAL2 e UAL3, appare opportuno precisare lo standard di conformità richiesto, indicando quali elementi debbano essere dimostrati dagli operatori per affrontare i rischi connessi ai regimi di sanzioni ed embarghi adottati da Paesi terzi e secondo quali modalità tali elementi debbano essere valutati nell'ambito dell'audit.

L'attenzione dovrebbe concentrarsi sull'effettiva capacità di eventuali misure restrittive adottate da Paesi terzi di incidere sul funzionamento del servizio all'interno dell'Unione europea. Un approccio fondato sulla valutazione concreta dei rischi e delle misure di mitigazione adottate risulterebbe maggiormente coerente con le finalità del quadro normativo.

La valutazione dovrebbe quindi verificare se una misura restrittiva di un Paese terzo possa concretamente essere imposta al servizio sottoposto ad audit o incidere sulla sua operatività nell'Unione, anziché basarsi esclusivamente su collegamenti societari o proprietari con soggetti stabiliti al di fuori dell'Unione.
Una maggiore precisione del criterio G.4 contribuirebbe a rafforzare la certezza giuridica, a rendere omogenea l'attività degli organismi di audit e a consentire ai provider di individuare e documentare adeguatamente le misure di mitigazione adottate.

9. **Principi per un quadro normativo efficace**

Per conseguire pienamente gli obiettivi del *Cloud and AI Development Act,* riteniamo che il quadro normativo dovrebbe ispirarsi ad alcuni principi fondamentali.

In primo luogo, la proporzionalità, affinché gli obblighi richiesti siano commisurati ai rischi e alla criticità dei servizi.

In secondo luogo, la neutralità tecnologica, che consente di valutare i risultati raggiunti piuttosto che prescrivere specifiche soluzioni tecnologiche.

Risultano inoltre essenziali la certezza giuridica e la chiarezza delle definizioni, delle procedure e dei criteri di audit, così come la possibilità di dimostrare la conformità attraverso evidenze tecni-

che e organizzative verificabili. Altrettanto importante è la promozione dell'apertura e dell'interoperabilità, attraverso il sostegno a standard aperti, open source, portabilità e cloud ibrido, elementi che contribuiscono in modo significativo all'autonomia strategica europea.

Infine, qualsiasi misura volta a rafforzare la sovranità digitale dovrebbe essere valutata anche alla luce del suo impatto sulla sicurezza e sulla resilienza complessiva delle infrastrutture e dei servizi.

L'applicazione congiunta di tali principi dovrebbe condurre a requisiti fondati sul rischio, orientati ai risultati e concretamente sottoponibili ad audit. In questo modo, il quadro europeo potrebbe tutelare il controllo sui dati e sui servizi senza introdurre restrizioni più ampie di quanto necessario né ridurre la capacità degli operatori di rispondere efficacemente agli incidenti di sicurezza.

10. **Considerazioni finali**

Alla luce delle osservazioni formulate, IBM ritiene che il *Cloud and AI Development Act* possa rappresentare un passaggio importante per rafforzare la competitività digitale europea, sostenere lo sviluppo dell'ecosistema del cloud e dell'intelligenza artificiale e accrescere la resilienza delle infrastrutture strategiche dell'Unione.

Per raggiungere pienamente tali obiettivi, appare essenziale che il quadro normativo garantisca chiarezza, prevedibilità e certezza giuridica, consentendo agli operatori di comprendere con precisione gli obblighi richiesti e le modalità attraverso cui dimostrare la conformità ai requisiti di sovranità previsti dalla normativa.

In particolare, appare opportuno circoscrivere la nozione di subfornitore ai soggetti direttamente coinvolti nell'erogazione del servizio sottoposto ad audit e definire con chiarezza il relativo perimetro, assicurando piena coerenza tra gli Allegati II e III.

È altresì necessario adottare un approccio proporzionato e basato sul rischio per il trattamento di metadati, telemetria e attività di supporto, distinguendo i dati dei clienti dai dati operativi e preservando la possibilità di ricorrere alle competenze necessarie per rispondere tempestivamente agli incidenti informatici.

I criteri applicabili a UAL2 e UAL3 dovrebbero essere fondati sul controllo operativo effettivo e su garanzie trasparenti e sottoponibili ad audit, evitando automatismi basati esclusivamente sulla struttura proprietaria, sulla nazionalità o sull'origine geografica delle componenti tecnologiche. Parallelamente, i criteri I.2 e G.4 dovrebbero essere precisati per assicurare proporzionalità, concreta applicabilità e certezza giuridica.

Riteniamo inoltre che la disciplina debba continuare a fondarsi su criteri proporzionati e tecnologicamente neutrali, orientati ai risultati e non alle caratteristiche formali dei fornitori. La capacità di assicurare controllo effettivo sui dati, protezione degli accessi, continuità operativa e resilienza dei servizi dovrebbe costituire il principale parametro di valutazione dell'autonomia e della sovranità digitale.

Particolare attenzione dovrebbe essere riservata alla promozione dell'interoperabilità, della portabilità dei dati e delle applicazioni, degli standard aperti e dei modelli open source. Questi elementi contribuiscono concretamente a rafforzare la sovranità digitale europea perché consento-

no a imprese e pubbliche amministrazioni di mantenere la libertà di scelta delle tecnologie e dei fornitori, riducendo il rischio di dipendenze tecnologiche e favorendo un mercato più competitivo e innovativo. Allo stesso tempo, è importante che gli obblighi introdotti dal quadro normativo non compromettano la capacità degli operatori di garantire elevati livelli di sicurezza e resilienza. Le attività di prevenzione, rilevazione e risposta agli incidenti informatici richiedono infatti l'accesso alle migliori competenze disponibili e la possibilità di adottare modelli operativi adeguati alla natura globale delle minacce cyber.

Merita infine attenzione il possibile impatto economico delle disposizioni previste dal quadro di sovranità sui soggetti pubblici e privati che acquistano servizi cloud. Requisiti particolarmente stringenti o formulati in modo da restringere significativamente il numero dei fornitori in grado di soddisfarli potrebbero infatti ridurre la concorrenza e tradursi in maggiori costi di acquisto e gestione dei servizi digitali. Tale aspetto assume particolare rilevanza per le pubbliche amministrazioni, che potrebbero essere chiamate a sostenere oneri aggiuntivi per l'accesso a servizi conformi ai livelli più elevati di sovranità, con possibili effetti sulle risorse disponibili per gli investimenti in innovazione, competenze e trasformazione digitale. Appare pertanto opportuno che la valutazione delle misure previste dal regolamento tenga conto anche del loro impatto sulla competitività del mercato, sulla disponibilità di soluzioni innovative e sul rapporto costi-benefici per gli utenti finali, inclusa la Pubblica Amministrazione.In conclusione, IBM ritiene che il rafforzamento della sovranità digitale europea debba fondarsi su un equilibrio tra sicurezza, innovazione, interoperabilità e libertà di scelta. Un quadro normativo chiaro, proporzionato e orientato ai risultati può contribuire a consolidare l'autonomia strategica dell'Europa, sostenere gli investimenti in infrastrutture e competenze digitali e favorire la competitività del sistema economico europeo.

In questa prospettiva, la sovranità digitale dovrebbe essere intesa come la capacità effettiva di garantire il controllo dei dati, la sicurezza e la continuità dei servizi, preservando al contempo apertura del mercato, concorrenza, interoperabilità e assenza di vincoli tecnologici che limitino la libertà di scelta degli utenti.

IBM conferma il proprio impegno a collaborare con le istituzioni nazionali ed europee per favorire lo sviluppo di un ecosistema del cloud e dell'intelligenza artificiale aperto, sicuro e resiliente, capace di sostenere la trasformazione digitale del Paese, la modernizzazione della Pubblica Amministrazione, la crescita delle imprese e la competitività dell'Europa nel lungo periodo.

Per ulteriori approfondimenti

Alessandra Santacroce, Direttore Government and Regulatory Affairs IBM Italia, email: alessandra_santacroce@it.ibm.com

Sara Marini, Public Affairs IBM Italia, email: sara.marini@it.ibm.com