POLICY BRIEF

POLLICINO & PARTNERS
AIDVISORY

La Proposta di Regolamento UE sullo sviluppo del Cloud e dell'IA (CADA): profili essenziali

Sofia Menici[1] e Rebecca Pupella[2]

Il 3 giugno scorso la Commissione Europea ha presentato la proposta di Regolamento Cloud and AI Development Act (la "Proposta"), volta ad istituire un quadro di misure per rafforzare l'ecosistema europeo del cloud e dell'intelligenza artificiale nell'Unione.

Partendo dal presupposto che cloud computing, intelligenza artificiale ("IA") e infrastrutture di calcolo sono risorse strategiche per la competitività, la resilienza, la sicurezza economica e l'autonomia tecnologica dell'Unione, la Proposta, che potrà essere oggetto di modifiche nell'ambito della procedura legislativa ordinaria, individua due principali criticità:

(i) la disponibilità limitata e geograficamente concentrata di capacità computazionale e di data centre nell'Unione;

(ii) la dipendenza dell'Unione da un numero limitato di fornitori cloud extra-UE, con conseguenti rischi in termini di accesso ai dati, continuità dei servizi ed autonomia operativa.

e persegue due obiettivi generali:

(i) rafforzare la competitività e la capacità innovativa dell'ecosistema europeo cloud e IA;

(ii) migliorare il funzionamento del mercato interno attraverso un quadro giuridico armonizzato volto ad aumentare resilienza e autonomia strategica dell'Unione.

In particolare, la Proposta interviene sulle seguenti aree principali, che verranno di seguito analizzate:

1. istituzione delle c.d. "*Cloud and AI Leadership Initiatives*" (Titolo II);
2. accelerazione dello sviluppo e della diffusione dei data centre nel territorio dell'Unione (Titolo III);
3. definizione di un quadro per soluzioni cloud e IA "sovrane", al fine di tutelare l'ordine pubblico e gli interessi strategici dell'UE, nonché ridurre le dipendenze tecnologiche provenienti da Paesi extra-UE (Titolo IV);
4. riforma del *procurement* pubblico in ambito cloud e IA, in ottica di una maggiore adozione dei servizi *cloud computing* e delle soluzioni *open source* da parte delle amministrazioni pubbliche (Titolo IV).

[1] Dottoressa in Diritto e Tecnologia, Pollicino AIdvisory.
[2] Advisor AI Governance & Cybersicurezza, Pollicino AIdvisory.

1. Cloud and AI Leadership Initiatives e misure di sviluppo (Titolo II)

Il Titolo II del CADA istituisce le *Cloud and AI Leadership Initiatives*, per promuovere ricerca, innovazione e capacità su larga scala nell'ecosistema cloud e IA europeo.

In particolare, gli aspetti più rilevanti riguardano:

(i) lo sviluppo di tecnologie avanzate per cloud, IA e data centre di nuova generazione ad alta efficienza energetica;

(ii) il rafforzamento delle infrastrutture cloud e data centre per sostenere l'autonomia tecnologica UE;

(iii) il potenziamento delle capacità europee in materia di IA avanzata, IA fisica e IA industriale, con particolare attenzione ai settori strategici quali sanità, energia, mobilità, automotive, manifattura, difesa, spazio, clima, ambiente e agrifood;

(iv) la promozione di piattaforme avanzate per l'adozione su larga scala di agenti IA e l'utilizzo diffuso di tecnologie cloud e IA nel settore pubblico.

La Proposta pone in capo agli Stati membri alcuni obblighi, in particolare:

(i) l'istituzione di centri di accelerazione per l'IA ("*Experience and Acceleration Centres for AI*") finalizzati a sostenere l'integrazione e l'ampliamento dei casi d'uso dell'IA nei settori industriali e pubblici strategici, accelerare l'adozione diffusa delle tecnologie cloud e di IA a livello regionale e locale, in particolare da parte di PMI, SMC e organismi del settore pubblico e sfruttare le infrastrutture pertinenti per accelerare lo sviluppo e la messa a punto dei modelli e dei sistemi di IA; e

(ii) l'adozione di strategie nazionali cloud e IA, includendo misure su infrastrutture, data centre e *procurement* innovativo.

2. Data centre acceleration zones (Titolo III)

Il Titolo III introduce le *data centre acceleration zones***,** ossia aree dedicate individuate dagli Stati membri per accelerare la realizzazione di data centre.

I punti più rilevanti riguardano:

(i) l'obbligo per ogni Stato membro di designare almeno una zona dedicata allo sviluppo di data centre entro sei mesi dall'entrata in vigore del Regolamento, tenendo conto della disponibilità energetica, connettività, e sostenibilità ambientale;

(ii) la semplificazione delle procedure autorizzative per la costruzione dei data centre all'interno delle zone designate, con tempi massimi pari a 12 mesi dalla presentazione della domanda completa;

(iii) la pianificazione del fabbisogno energetico e infrastrutturale delle suddette zone in capo agli Stati membri, con particolare attenzione a energie pulite e recupero del calore residuo;

(iv) il coordinamento tra autorità nazionali, regionali e locali competenti e operatori delle infrastrutture energetiche e di comunicazione elettronica, nella definizione e gestione delle zone di accelerazione.

La Proposta precisa, poi, che la Commissione può qualificare alcuni progetti di data centre come strategici (*strategic projects*), in presenza di requisiti quali innovazione, sostenibilità, supporto a funzioni pubbliche essenziali o risposta a carenze infrastrutturali.

3. Quadro Europeo per la sovranità del Cloud computing e Livelli di garanzia dell'Unione (Titolo IV)

Il Titolo IV della Proposta istituisce un Quadro Europeo per la sovranità del *cloud computing* (*Union cloud computing sovereignty framework*), articolato in quattro livelli di garanzia dell'Unione[3].

I fornitori di servizi *cloud computing* devono soddisfare i requisiti elencati nell'Allegato II della Proposta per poter erogare servizi cloud alle istituzioni UE ed alle amministrazioni pubbliche.

È, poi, prevista, agli artt. 17 ss, una specifica procedura di riconoscimento e valutazione di conformità dei fornitori di servizi cloud articolata su quattro livelli di garanzia.

In particolare:

(i) per quanto concerne quella di primo livello, il fornitore di servizi *cloud computing* effettua un'autovalutazione della conformità ai requisiti applicabili di cui all'Allegato II della Proposta e rilascia la dichiarazione UE di conformità, la rende pubblica e la trasmette all'autorità nazionale competente ai fini del riconoscimento. Per i fornitori che siano PMI, la proposta prevede una deroga: la dichiarazione UE di conformità è direttamente e automaticamente riconosciuta in tutti gli Stati membri, senza necessità di previo riconoscimento da parte dell'autorità nazionale competente;

(ii) relativamente, invece, ai livelli 2, 3 e 4, il riconoscimento da parte dell'autorità nazionale competente è subordinato ad un audit svolto da un organismo di

[3] Ai sensi dell'Allegato II della proposta, i quattro livelli di garanzia dell'Unione sono sintetizzabili come segue:
Livello 1: i dati devono essere trattati e conservati in infrastrutture situate nel territorio dell'Unione; **Livello 2**: il fornitore deve dimostrare la propria indipendenza da Paesi terzi e garantire trasparenza sulla propria catena di fornitura software;
Livello 3: il fornitore deve essere controllato da soggetti dell'Unione europea e soddisfare ulteriori requisiti, tra cui criteri relativi al personale impiegato; la Commissione può tuttavia ammettere fornitori provenienti da determinati Paesi terzi che rispettino specifiche condizioni;
Livello 4: il fornitore deve garantire piena trasparenza e controllo della propria catena di fornitura software, nonché l'assenza di interferenze da parte di Paesi terzi.

revisione qualificato e indipendente, che presenta una relazione ed un parere di audit positivi o negativi.

Il riconoscimento produce effetti in tutta l'Unione Europea e, ai sensi dell'articolo 22 della Proposta, la Commissione provvede ad istituire un registro pubblico dei servizi riconosciuti.

Per quanto concerne fornitori extra-UE, ai sensi dell'articolo 18, la Proposta prevede che la Commissione possa identificare Paesi terzi i cui fornitori di servizi cloud possono accedere al livello 3 di garanzia, purché tali Paesi garantiscano:

(i) un livello adeguato di protezione dei dati personali mediante specifica decisione di adeguatezza ai sensi dell'articolo 45 del Regolamento UE 2016/679[4];
(ii) l'assenza di misure che consentano alle autorità nazionali di esercitare forme di controllo sui fornitori di servizi cloud incompatibili con le norme dell'Unione in materia di accesso lecito ai dati non personali;
(iii) l'assenza di misure che possano compromettere la continuità o l'erogazione dei servizi cloud, ovvero imporre ai fornitori l'applicazione di sanzioni, embarghi o altre restrizioni non conformi al diritto dell'Unione o degli Stati membri;
(iv) l'assenza di misure che ostacolino la fornitura di tecnologie e servizi cloud all'avanguardia;
(v) il mantenimento di un mercato aperto ai servizi di *cloud computing* dell'Unione;
(vi) condizioni di accesso non discriminatorie ed equivalenti alle procedure di appalto pubblico per i fornitori di servizi cloud nell'Unione.

Agli Stati membri, poi, è affidato il compito di determinare sanzioni effettive, proporzionate e dissuasive, applicabili in caso di violazione di quanto contenuto nella Proposta. Si precisa che i destinatari dei servizi cloud hanno diritto al risarcimento per eventuali danni o perdite derivanti dalla violazione degli obblighi da parte del fornitore.

Agli stessi Stati membri spetta altresì il compito di designare una o più autorità nazionali competenti entro un anno dall'entrata in vigore della Proposta, con poteri investigativi e di *enforcement* (richiesta di informazioni, ispezioni, ordini di cessazione, sanzioni).

Si chiarisce che la competenza esclusiva per l'*enforcement* spetta allo Stato membro in cui il fornitore dei servizi di *cloud computing* ha il proprio stabilimento principale. Sono previsti, inoltre, meccanismi di assistenza reciproca e cooperazione transfrontaliera tra le autorità competenti.

[4] L'art. 45 del Regolamento (UE) 2016/679 prevede che il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale sia ammesso senza autorizzazioni specifiche quando la Commissione abbia accertato, mediante decisione di adeguatezza, che il destinatario garantisce un livello di protezione adeguato.

Quanto al ruolo della Commissione, la Proposta attribuisce ad essa significativi poteri di attuazione tramite atti delegati, i quali possono disciplinare, *inter alia*, le modalità di svolgimento degli audit, i requisiti e le competenze degli organismi di revisione, i modelli standard per la redazione delle relazioni di audit.

Con riguardo alle entità soggette alla Direttiva (UE) 2022/2555 ("NIS2"), poi, la Proposta introduce un ulteriore livello di valutazione del rischio rispetto a quello già previsto dalla NIS2, focalizzato non sulla sicurezza informatica in senso tecnico ma sui profili di sovranità, indipendenza operativa e resilienza dei fornitori di servizi cloud. In particolare, gli artt. 29 e 30 della Proposta prevedono che gli Stati membri e gli enti dell'Unione effettuino valutazioni del rischio per individuare le attività di settore pubblico che rientrano nei settori di cui agli Allegati I e II della NIS2 (oltre alle aree di sicurezza nazionale, difesa, giustizia e ordine pubblico), al fine di determinare se per tali attività sia necessario l'utilizzo di servizi cloud certificati ai livelli di garanzia 2, 3 o 4. L'articolo 31 della Proposta estende questo meccanismo — su base facoltativa — anche alle entità private rientranti nell'Allegato I della NIS2: tali soggetti, qualora non siano enti pubblici, possono condurre valutazioni d'impatto analoghe a quelle previste per le amministrazioni pubbliche all'articolo 29.

4. Riforma del procurement pubblico in ambito cloud e IA (Titolo IV)

Relativamente al *procurement*, la Proposta chiarisce che nelle procedure di appalto per servizi cloud e sistemi di IA innovativi, le amministrazioni aggiudicatrici devono includere criteri qualitativi non basati sul prezzo per valutare il contributo allo sviluppo dell'ecosistema europeo (a titolo esemplificativo, l'integrazione di tecnologie sviluppate nell'Unione, uso di componenti *hardware* progettati o prodotti nell'Unione).

E' previsto, inoltre, come obiettivo indicativo, che almeno il 25% degli appalti pubblici per servizi cloud e sistemi di IA sia assegnato a PMI innovative.

Viene, inoltre, prevista l'istituzione dell'*EuroCloud Federation*, ossia una federazione a partecipazione volontaria, gestita dalla Commissione Europea e aperta a enti e amministrazioni pubbliche europee per la condivisione di infrastrutture cloud e data centre.

La Proposta introduce, poi, agli articoli 41 ss, una serie di misure volte a rafforzare l'adozione di soluzioni *open source* nel settore pubblico. In particolare, le amministrazioni pubbliche europee e nazionali sono chiamate a privilegiare soluzioni basate su standard aperti e *software open source* rispetto a quelle proprietarie. A tal fine, la Proposta promuove la condivisione e il riutilizzo del *software* sviluppato con risorse pubbliche, istituisce un Catalogo europeo delle soluzioni *open source* quale punto unico di accesso alle risorse disponibili e crea una rete degli *Open Source Programme Offices* (OSPO) nazionali, con il compito di favorire il coordinamento, la cooperazione e lo scambio di buone pratiche tra gli Stati membri.