**CONSORZIO ITALIA CLOUD**
Sede in ROMA – Largo di Torre Argentina n.11
Registro delle Imprese di ROMA e codice fiscale 16295181008

**Alla I Commissione Affari Costituzionali - Camera dei deputati**
*alla. c.a. del Presidente On. Nazario Pagano*
*e degli Onorevoli Deputati*

**Alla IX Commissione Trasporti - Camera dei deputati**
*alla c.a. del Presidente On. Salvatore Deidda*
*e degli Onorevoli Deputati*

inviato via email a: com_trasporti@camera.it

Roma, 16 Luglio 2024

# Contributo del Consorzio Italia Cloud

## nell'ambito dell'esame dell'Atto del Governo n. 164, recante recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (cd. NIS2 )

Illustrissimi Presidenti, Onorevoli Deputati

Il Consorzio Italia Cloud ringrazia dell'opportunità concessa di fornire un contributo scritto nell'ambito dell'esame dell'Atto del Governo in oggetto e si dichiara disponibile ad un'eventuale audizione per approfondire ulteriori aspetti si rendessero necessari nell'analisi delle misure per un livello comune elevato della cybersicurezza nell'Unione.

## 1 - PRESENTAZIONE CONSORZIO ITALIA CLOUD

Costituto nell'agosto 2021 da aziende italiane che operano nella fornitura di servizi di Cloud Computing, il Consorzio Italia Cloud ha tra le sue finalità statutarie quella di sviluppare l'offerta e le competenze nazionali già presenti negli operatori privati e nella pubblica amministrazione per supportare la digitalizzazione e l'adozione di tecnologie cloud nelle realtà private e nel settore pubblico. Il Consorzio si prefigge inoltre di promuovere la gestione dei dati strategici nazionali in ossequio alle normative di

sicurezza e di privacy, finalizzate al rispetto di principi di sovranità digitale, interoperabilità e trasparenza.

Prime aziende ad aver aderito al Consorzio Italia Cloud sono state **Seeweb**, **Sourcesense**, **Infordata**, **BabylonCloud**, **ConsorzioEHT** e **Netalia**, tutte attive nel mercato cloud nazionale, ognuna con la propria specifica focalizzazione.

Il Consorzio Italia Cloud, nato dalla confluenza naturale di realtà che condividono gli stessi valori e lo stesso approccio al mercato è aperto a tutte le aziende italiane che intendono contribuire a questo modello sulla base degli stessi principi. Infatti, da dicembre 2021, anche **Insiel S.p.A**, la società in-house della Regione Friuli Venezia Giulia, ha deciso di unirsi al Consorzio e di contribuire alla sua attività di difesa delle imprese e delle competenze italiane del settore.

## 2 – LA DIFESA CIBERNETICA E LA DIPENDENZA TECNOLOGICA DA PRODOTTI E SERVIZI

Le recenti tensioni geopolitiche stanno ponendo in seria discussione le attività tradizionali di difesa dagli attacchi informatici che - in un contesto di guerra ibrida, anche informatica - si aggiungono e si sommano ai rischi che siamo abituati a fronteggiare su base giornaliera.

Un contesto di conflitto tra Stati come quello che stiamo vivendo, ha reso il cyberspazio un luogo ancora più difficile da difendere e quindi da governare. Il furto di dati, l'interruzione delle comunicazioni, delle forniture di energia e gas, o la sospensione delle elezioni o dei cicli di vaccinazione, sappiamo essere capaci di creare disservizi talmente gravi da mettere in pericolo l'ordine pubblico e la sicurezza degli Stati. Un atteggiamento solamente reattivo potrebbe rivelarsi inadeguato a gestire le nuove minacce - alcune di esse finora sconosciute e quindi non sufficientemente ponderate.

Il crescente isolamento della Russia sulla scena internazionale ed il rischio di attacchi contro attori industriali nostri alleati oltreoceano, pongono la necessità di ponderare meglio il rischio di affidare i dati strategici nazionali a fornitori di tecnologie estere nel settore del cloud computing. **Nel breve termine - a fronte anche delle novità introdotte dalla disciplina europea della direttiva NIS2 - andrebbe considerata parallelamente una strategia di politica interna per la diversificazione delle soluzioni cloud a cui si affidano i servizi della nostra Pubblica Amministrazione, in modo tale che non resti concentrata su soluzioni tecnologiche extraeuropee.**

Questo perché finora non sembrano essere stati presi in sufficiente considerazione gli impatti indiretti della sospensione di servizi erogati da fornitori esteri extraeuropei quando soggetti ad attacchi informatici. I recenti accadimenti di guerra stanno mostrando l'alto rischio di fare affidamento su pochi fornitori critici esteri in un'economia globalizzata.  Per questo motivo tutti gli operatori si oppongono ad accordi esclusivi con un singolo fornitore.

Nel mercato della telefonia ad esempio, si registra una certa resilienza - anche se a volte solo teorica - dovuta principalmente a scorte di apparati che vengono fatte dagli operatori ed ai cicli di sostituzione degli apparati molto più lunghi rispetto ad altri settori dell'innovazione.

Non è così per il mercato del cloud computing dove la resilienza non è garantita quando ci si affida a provider di servizi esteri che volontariamente o sotto attacco informatico, potrebbero interrompere le forniture. **È nell'immediatezza degli effetti distruttivi che va quindi colta la differenza principale tra il venir meno di un servizio e il venir meno della disponibilità futura di un apparato.**

Il problema della disponibilità del servizio a fronte di un contesto di crisi internazionale e di aumento degli attacchi cibernetici - come quello in cui viviamo - ha reso del tutto insicura la proposta di affidare le funzioni più critiche a partner tecnologici extraeuropei - quand'anche essi garantiscano contrattualmente la territorialità dei dati (cd. Localizzazione) nel mercato interno.

Ridurre la dipendenza da prodotti o servizi extraeuropei, sviluppare un'economia interna della conoscenza, il rafforzamento delle regole sulla cybersicurezza sono finalità che possono essere perseguite solo se si realizzano contemporaneamente le politiche nazionali volte a conseguirle. Avere una valutazione della propria "resilienza" cibernetica, significa predisporre dei test in tal senso, ma prima di farlo, occorrerebbe a nostro avviso ridurre fino ad eliminare la dipendenza dai fornitori globali extra-europei di tecnologie cloud computing.

## 3 - ANALISI D'IMPATTO DELL'ART.26 – Giurisdizione e territorialità

L'analisi del testo di cui all'Art.26 in esame suggerisce elementi di approfondimento che andremo di seguito ad evidenziare in neretto ed a dettagliare in termini di impatto sulla nostra giurisdizione.

Articolo 26 - Giurisdizione e territorialità

**1. Le entità che rientrano nell'ambito di applicazione della presente direttiva sono considerate soggette alla giurisdizione dello Stato membro in cui sono stabilite**, ad eccezione dei casi:
(A)
fornitori di reti pubbliche di comunicazioni elettroniche o fornitori di servizi di comunicazioni elettroniche accessibili al pubblico, che sono considerati ricadenti nella giurisdizione dello Stato membro in cui forniscono i loro servizi;

(B)
Fornitori di servizi DNS, registri di nomi TLD, entità che forniscono servizi di registrazione di nomi di dominio, **fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti per la distribuzione di contenuti, fornitori di servizi gestiti, fornitori di servizi di sicurezza gestiti, nonché fornitori di mercati online, motori di ricerca online o piattaforme di servizi di social network, che sono considerati rientranti nella giurisdizione dello Stato membro in cui hanno la loro sede principale nell'Unione ai sensi del paragrafo 2;**

(C)
enti della pubblica amministrazione, che si considerano ricadenti nella giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini della presente direttiva, un'entità di cui al paragrafo 1, lettera b), si considera abbia la sua sede principale nell'Unione nello Stato membro in cui vengono prevalentemente prese le decisioni relative alle misure di gestione del rischio di sicurezza informatica. Se tale Stato membro non può essere determinato o se tali decisioni non sono prese nell'Unione, la sede principale si considera nello Stato membro in cui vengono svolte le operazioni di sicurezza informatica. Se tale Stato membro non può essere determinato, la sede principale si considera nello Stato membro in cui l'entità interessata ha la sede con il numero più elevato di dipendenti nell'Unione.
3. Se un'entità di cui al paragrafo 1, lettera b), non è stabilita nell'Unione, ma offre servizi all'interno dell'Unione, essa designa un rappresentante nell'Unione. Il rappresentante deve essere stabilito in uno degli Stati membri in cui vengono offerti i servizi. Tale entità è considerata rientrante nella giurisdizione dello Stato membro in cui è stabilito il rappresentante. In assenza di un rappresentante nell'Unione designato ai sensi del presente paragrafo, qualsiasi Stato membro in cui l'entità fornisce servizi può intraprendere azioni legali contro l'entità per violazione della presente direttiva.
4. La designazione di un rappresentante da parte di un soggetto di cui al paragrafo 1, lettera b), non pregiudica le azioni legali che potrebbero essere promosse nei confronti del soggetto stesso.
**5. Gli Stati membri che hanno ricevuto una richiesta di assistenza reciproca in relazione a un'entità di cui al paragrafo 1, lettera b), possono, nei limiti di tale richiesta, adottare misure di vigilanza e di esecuzione appropriate nei confronti dell'entità interessata che fornisce servizi o che dispone di una rete e di un sistema informativo sul loro territorio.**

A nostro avviso merita grande attenzione la fattispecie contemplata nella norma dell'art.26 paragrafo 1 lettera B), di fornitura di servizi di cloud computing in Italia da parte di un soggetto considerato sotto la giurisdizione di un altro Stato Membro o i cui sistemi informativi e di rete sono ubicati sul territorio di altri Stati membri, ma fornisce servizi sul territorio nazionale italiano. Le criticità che potrebbero emergere sono varie e la Direttiva si limita a prevedere un coordinamento tra Autorità europee preposte che mantengono poteri di vigilanza a livello locale (paragrafo 5).

**È chiarissimo l'intento del Legislatore di non limitare la libertà di circolazione dei beni e servizi nel territorio eurounitario ma ricordiamo che potrebbero anzitutto verificarsi dei casi noti come "forum shopping", ovvero la scelta della sede principale sulla base di ragioni opportunistiche al fine di garantirsi una giurisdizione più vantaggiosa.** Ricordiamo infatti che la Direttiva NIS2 impone un "livello comune" di misure che sono da considerarsi obbligatorie, ovvero un "set minimo" a cui devono uniformarsi tutti gli Stati Membri che però restano liberi di poter aumentare in maniera necessaria, proporzionata e motivata le eventuali misure aggiuntive che dovessero rendersi necessarie per meglio perseguire gli obiettivi di elevata sicurezza cibernetica.

Alcuni esempi di casi analoghi, si possono ritrovare nello stabilimento principale quando viene eletto nel territorio degli Stati che offrono una fiscalità di vantaggio rispetto ad altri Stati. Nel caso della disciplina ora in discussione, si potrebbe verificare l'ipotesi per cui un operatore pan-europeo, molto più spesso extra-europeo e con dimensione globale nell'offerta di servizi di Cloud Computing, elegga come sede principale lo Stato Membro che gli garantisca condizioni migliorative rispetto ad altri. E' una prerogativa che peraltro viene negata agli operatori più piccoli che operano in un solo mercato nazionale e che sicuramente saranno soggetti alla giurisdizione locale.

**Residuano tuttavia ulteriori perplessità in merito all'efficacia ed all'immediatezza dell'assistenza reciproca tra le diverse Autorità NIS** nel momento in cui dovesse esserci un grave attacco informatico ad un Operatore pan-europeo o extra-europeo che gestisca dati della Pubblica Amministrazione italiana, ma avendo la sede stabile per ipotesi in Ungheria o in Irlanda o in un altro Stato Membro, comporterebbe che la giurisdizione su un incidente di sicurezza grave che coinvolga i nostri dati critici o strategici, sarebbe demandata ad un altro Stato europeo e non all'Italia.

**Quando un Paese come l'Italia affida i dati critici ad operatori esteri extra-europei – finanche quando fossero in partnership con operatori locali ma con la sede stabile in un altro Stato Membro - occorrerà valutare fin da principio che potrebbe perderne il controllo. Per sempre.**

(Sul punto degli effetti negativi immediati del venir meno di un servizio richiamiamo quanto supra al paragrafo n.2 – LA DIFESA CIBERNETICA E LA DIPENDENZA TECNOLOGICA DA PRODOTTI E SERVIZI)

Il vantaggio apparente che il dato sia localizzato nel territorio italiano, non potrà per questo mai soddisfare, da solo, il requisito di sovranità per i dati strategici della PA. E questo, a maggior ragione, nel rinnovato panorama geopolitico che stiamo vivendo, perché i dati crittografati potrebbero non essere mai più disponibili o accessibili. **È un tema di grande impatto nella discussione in corso a Bruxelles, ed è sostanzialmente la causa del ritardato accordo sul nuovo Schema Europeo di Cybersicurezza (cd. EUCS *"European Cybersecurity Certification Scheme for Cloud Services"*)** poiché si rende sempre più necessario affidare la gestione dei dati strategici della PA ad operatori nazionali, in un mercato globale che resta dominato da cinque grandi operatori "Bigtech", ovvero giganti tecnologici, tutti extra-europei, dotati di un'elevata rappresentanza di interessi e di altrettanta capacità di influenza delle decisioni.

## 4 - LA VALORIZZAZIONE DELLE IMPRESE ITALIANE ATTIVE NEL CLOUD E NELLA CYBERSECURITY

Uno degli ingredienti principali per rafforzare la nostra cybersicurezza è quello di sviluppare competenze e conoscenze a livello locale, grazie all'investimento dei privati ed al supporto del settore pubblico e delle Autorità preposte. Affinché ciò possa avvenire si è discusso molto di finanziamento di Ricerca, Sviluppo e Innovazione (R&S&I) a livello centrale. Riteniamo che sia opportuno che – nel raggiungere questo obiettivo - non vengano eradicate competenze locali a favore di un solo polo centrale nazionale attrattivo di talenti.

**Per questi motivi non crediamo nella creazione di un "campione nazionale" nella cybersicurezza o di pochi soggetti che a vari livelli possano primeggiare con altri operatori europei. Crediamo invece che sia opportuno mantenere e**

**sviluppare un giusto ecosistema industriale distribuito su tutto il territorio nazionale**, non solo attraverso la creazione di start-up, ma facendo crescere le PMI esistenti e che già oggi offrono servizi tecnologici avanzati in ambito cloud e cybersecurity, ivi comprese le in house regionali che da sempre sono il riferimento territoriale dei cittadini che fruiscono di servizi pubblici avanzati.

****

Auspichiamo che queste considerazioni del Consorzio Italia Cloud possano aprire una riflessione ulteriore sull'opportunità di perseguire un livello elevato di cybersicurezza favorendo la crescita di operatori locali nazionali di servizi cloud, in modo da rafforzare quella che è l'industria italiana più legata alle conoscenze ed alle competenze nel settore della sicurezza cibernetica a favore della nostra economia digitale.

Rimaniamo fin da subito a disposizione per un'eventuale audizione o per la fornitura di ulteriori informazioni qualora si rendessero necessarie a valle dell'invio del presente contributo che è da considerarsi interamente accessibile e pubblicabile integralmente sul sito istituzionale della Camera dei Deputati.

L'occasione ci è cara per porgervi i nostri cordiali saluti,

Michele Zunino
Presidente

Consorzio Italia Cloud