
Progettare il futuro digitale dell'Europa

Le fondamenta per un'infrastruttura cloud e AI europea.

aruba.it

S.
C
O
N
C
E
P
T

Il posizionamento europeo di Aruba

Questo paper nasce con un'intenzione precisa: chiarire come Aruba intende il proprio ruolo nell'ecosistema digitale europeo.

Il posizionamento dell'azienda si articola attorno al concetto di operatore europeo, non sovrano: un'identità che esprime un'appartenenza geografica, normativa e istituzionale concreta, non un'aspirazione all'isolamento tecnologico, concetto che spesso ruota intorno alla parola "sovranità".

Quest'ultima, infatti, pur rappresentando un termine rilevante nel dibattito politico e regolatorio, porta con sé implicazioni di autonomia, indipendenza e autosufficienza che non rispecchiano la visione di Aruba.

Scegliere Aruba, infatti, significa operare all'interno di un ecosistema di scelta

europeo: infrastrutture radicate sul territorio UE, governance allineata al quadro normativo comunitario, personale soggetto esclusivamente alla legge italiana ed europea.

Non si tratta di chiudersi all'innovazione globale, ma di poterla integrare su fondamenta trasparenti, governabili e resilienti.

È questa la differenza tra un posizionamento europeo, che parla di **appartenenza, responsabilità e fiducia**, e un posizionamento sovranista, che parla di controllo esclusivo e indipendenza da sistemi esterni. Le pagine che seguono analizzano le fondamenta infrastrutturali, normative e architetturali di questo modello.

Quando il cloud computing entrò nel mondo enterprise, le organizzazioni lo accolsero con un mix di entusiasmo e cautela. La promessa era forte: infrastrutture scalabili, distribuzione rapida dei servizi e la possibilità di innovare senza i vincoli degli ambienti IT tradizionali. Eppure, anche in quella fase iniziale, la maggior parte delle organizzazioni non migrò immediatamente l'intero patrimonio digitale verso il cloud.

Emersero invece modelli architetturali pragmatici. Ad esempio i sistemi core, quelli che gestivano dati sensibili, processi critici o proprietà intellettuale strategica, rimasero generalmente on premise, all'interno di infrastrutture completamente controllate dall'organizzazione, mentre i carichi di lavoro più periferici come ambienti di sviluppo, piattaforme di test, strumenti di collaborazione e applicazioni non critiche, iniziarono a spostarsi verso il cloud pubblico per beneficiare di agilità e scalabilità.

Questo equilibrio tra controllo e flessibilità divenne uno dei tratti distintivi della prima fase di adozione del cloud.

Oggi una dinamica simile sta riemergendo con l'AI e la sua integrazione negli ambienti operativi delle organizzazioni. Dopo anni dominati da sperimentazioni e proof of concept, le tecnologie AI stanno entrando in produzione e iniziano a influenzare processi core nelle imprese e nelle amministrazioni pubbliche. In questa transizione, quindi, la domanda non è più semplicemente quali modelli o strumenti adottare piuttosto sono da rivalutare le fondamenta infrastrutturali su cui queste tecnologie operano.

Dati sensibili, applicazioni strategiche e processi decisionali critici richiedono sempre più ambienti in grado di garantire governance, chiarezza giurisdizionale e trasparenza operativa. Allo stesso tempo, le piattaforme hyperscale continuano a offrire capacità senza pari in termini di potenza computazionale, servizi AI avanzati e scalabilità globale.

Ciò che sta emergendo è una nuova ricerca di equilibrio che richiama la prima era del cloud, ma in un contesto digitale molto più complesso.

Concetti come **governance digitale**, **residenza dei dati** e **repatriation** dei workload non rappresentano un arretramento rispetto al modello cloud. Riflettono piuttosto l'esigenza crescente di bilanciare l'agilità delle infrastrutture hyperscale con la governance, il controllo e l'autonomia tecnologica di lungo periodo necessari per gli asset digitali strategici.

Le organizzazioni stanno inoltre adottando approcci pragmatici come il minimum viable sovereignty, concentrandosi sui controlli più critici a livello di infrastruttura, dati e applicazioni per bilanciare requisiti di governance e fattibilità operativa.

Per le imprese e le amministrazioni europee, non si tratta più di un dibattito puramente tecnico o legale in quanto **il tema della localizzazione del dato sta diventando parte integrante della strategia digitale**, influenzando competitività, resilienza, scelte di sourcing, continuità operativa e adozione dell'AI su larga scala. Man mano che i sistemi digitali diventano centrali per la creazione di valore, la domanda su chi governa le fondamenta sottostanti diventa imprescindibile **per innovare ed evolvere nel tempo**.

Sommario

01 Le fondamenta dell'Europa digitale	3
02 Compliance: l'ossatura regolatoria	6
03 Resilienza, interoperabilità e infrastrutture aperte	10
04 Controllo strategico e il paradosso Compute-Compliance	13

CAPITOLO 01

Le fondamenta dell'Europa digitale

La governance del dato viene spesso descritta come un obiettivo politico, ma nella pratica è innanzitutto una condizione architeturale: è un sistema stratificato di controlli che determina chi governa l'infrastruttura digitale, dove risiedono i dati e come i sistemi tecnologici evolvono nel tempo. Ne consegue che invece di un principio astratto o uno slogan normativo, è il risultato di scelte progettuali concrete applicate ai diversi livelli dello stack digitale. Può essere compresa come una questione di fondamenta: man mano che gli ambienti digitali si espandono, tra dati, applicazioni, modelli di intelligenza artificiale e servizi interconnessi, la qualità e la reattività di tali fondamenta diventano decisive. Infatti governance, resilienza e chiarezza giurisdizionale non emergono negli strati superficiali dello stack: dipendono da come l'infrastruttura sottostante è stata progettata e governata fin dall'inizio.

Il primo livello è l'**infrastruttura fisica**. I data center rappresentano l'elemento fondativo della localizzazione del dato perché determinano dove risiedono fisicamente dati e servizi, il punto di partenza da cui è possibile stabilire governance, supervisione e chiarezza giurisdizionale.

Quando le infrastrutture sono progettate, operate e governate all'interno del quadro normativo europeo, le organizzazioni ottengono certezza sui riferimenti legali applicabili e sulla supervisione operativa. Senza questo, l'autonomia digitale rimane largamente teorica. In termini pratici, il controllo digitale inizia dall'infrastruttura che ospita i carichi di lavoro digitali.

Da questa base emerge il secondo livello: **l'architettura cloud**. Nell'ultimo decennio, il paradigma dominante è passato da modelli infrastrutturali centralizzati a modelli ibridi e multi cloud. Queste architetture consentono alle organizzazioni di combinare la scalabilità e l'innovazione degli hyperscaler con infrastrutture che rimangono sotto governance regionale o organizzativa. Le architetture ibride diventano così il meccanismo attraverso cui le organizzazioni riconciliano agilità e requisiti di governance per i workload strategici.

Un terzo livello riguarda la **governance dei dati**: la capacità di determinare dove i dati sono archiviati, sotto quale giurisdizione vengono trattati e come si muovono tra le infrastrutture. Nel contesto europeo, la residenza e la tracciabilità dei dati non sono semplici considerazioni operative: sono requisiti fondamentali legati alla protezione della privacy, agli obblighi di cybersecurity e alla responsabilità regolatoria.

L'Intelligenza Artificiale aggiunge un livello critico che amplifica queste questioni strategiche e riguarda l'infrastruttura e la governance dell'AI. Infatti i sistemi di AI si basano su grandi dataset, capacità computazionale specializzata come le GPU e flussi di dati continui tra training, inferenza e operatività. Man mano che le organizzazioni integrano l'AI nei processi core, l'infrastruttura di supporto determina il loro percorso tecnologico: prossimità dei dati, accesso alla capacità GPU e trasparenza dei flussi informativi diventano fattori decisivi per la conformità e la governance.

Questa prospettiva stratificata riflette anche una trasformazione più ampia nel modo in cui l'infrastruttura digitale viene percepita. I data center non sono più semplici strutture che ospitano server, bensì asset strategici in cui convergono molteplici dimensioni: disponibilità energetica, connettività ad alte prestazioni, framework di sicurezza, resilienza operativa e considerazioni normative.

In Aruba, la sostenibilità dell'infrastruttura digitale è un fattore strategico. I moderni data center europei si basano sempre più su fonti energetiche rinnovabili e sistemi di raffreddamento ad alta efficienza, garantendo che la crescita dei carichi di lavoro cloud e AI non avvenga a scapito della responsabilità ambientale.

Le infrastrutture in grado di sostenere workload AI avanzati sono le stesse che supportano l'autonomia digitale di lungo periodo. Per le organizzazioni che operano nel contesto regolatorio ed economico europeo, sapere dove sono localizzati i propri dati non implica isolamento dall'innovazione globale bensì rappresenta la capacità di integrare tecnologie esterne all'interno di infrastrutture che rimangono trasparenti, governabili e resilienti nel tempo. In questo senso, una governance europea non riguarda la limitazione delle scelte, ma il preservare le condizioni strutturali che permettono alle organizzazioni di mantenere controllo e autonomia nella propria evoluzione digitale.

La rilevanza strategica dell'infrastruttura digitale è influenzata anche dalle sue dimensioni energetiche, industriali e regolatorie. I carichi di lavoro AI sono altamente intensivi dal punto di vista computazionale e strettamente legati alla disponibilità di energia affidabile e sostenibile. Allo stesso tempo, il controllo sull'infrastruttura digitale è diventato un elemento di competitività economica e resilienza tecnologica.

In definitiva, **un'infrastruttura europea non serve solo a proteggere ciò che è critico oggi, ma a preservare le condizioni che permetteranno alle organizzazioni di adattarsi a ciò che diventerà critico domani.**

Perché è importante per imprese e pubbliche amministrazioni conservare il proprio dato in Europa

L'importanza di una governance europea emerge con particolare chiarezza se osservata dalla prospettiva delle imprese e delle amministrazioni pubbliche.

Per le **aziende**, è sempre più legata alla capacità di mantenere controllo architetturale sui workload strategici, proteggere i dati sensibili, diversificare le strategie di sourcing ed evitare dipendenze strutturali che potrebbero limitare le scelte future. Porta inoltre maggiore prevedibilità in termini di compliance, costi, continuità operativa ed evoluzione dell'infrastruttura, soprattutto mentre i sistemi di AI vengono integrati nei processi core.

In ultima analisi, la localizzazione del dato e la sua governance diventa un fattore competitivo, consentendo alle organizzazioni di rispondere con maggiore flessibilità ai cambiamenti di mercato, ai requisiti normativi e alle opportunità strategiche.

Per le **amministrazioni pubbliche**, la posta in gioco è ancora più alta.

Il controllo sui sistemi digitali riguarda la protezione dei dati dei cittadini, la continuità dei servizi essenziali e la garanzia che le infrastrutture digitali critiche operino all'interno di quadri giurisdizionali e di sicurezza chiari.

In entrambi i casi, non si tratta di una funzionalità da aggiungere a valle, ma di una condizione fondativa che determina se l'innovazione può essere adottata con sufficiente **fiducia, controllo e resilienza**.

Per questo motivo, le organizzazioni e le pubbliche amministrazioni cercano sempre più partner in grado di interpretare la europeicità non come un semplice requisito di compliance, ma come **un modello infrastrutturale costruito su fondamenta governabili**.

La prospettiva UE: le dimensioni della sovranità digitale

Sovranità giurisdizionale e strategica:

controllo su dove opera l'infrastruttura e sotto quali quadri legali sono governati i servizi digitali.

Sovranità dei dati e dell'AI:

capacità di gestire localizzazione, accesso e utilizzo dei dati, garantendo tracciabilità, protezione e un'adozione dell'AI conforme.

Sovranità tecnologica:

uso di standard aperti, interoperabilità e architetture componibili per evitare dipendenze da ecosistemi chiusi.

Sovranità dell'ecosistema e operativa:

supply chain resilienti, provider affidabili e infrastrutture sostenibili che supportano l'autonomia digitale di lungo periodo.

CAPITOLO 02

Compliance: l'ossatura regolatoria

Se la localizzazione del dato è, in ultima analisi, una questione architeturale, la compliance fornisce il quadro normativo che determina come tale architettura deve essere progettata.

Negli ultimi dieci anni, l'Unione Europea ha costruito uno dei sistemi di governance più completi per l'economia digitale, introducendo norme che riguardano protezione dei dati, cybersecurity, resilienza operativa e, più recentemente, Intelligenza Artificiale.

In questa prospettiva, l'Unione Europea non considera la sovranità come un principio unico, ma come un insieme di dimensioni interdipendenti: controllo giurisdizionale, governance dei dati, trasparenza tecnologica, resilienza operativa e fiducia a livello di ecosistema. Il quadro europeo emergente va quindi oltre la sola protezione dei dati. Collega localizzazione dell'infrastruttura, obblighi di cybersecurity, interoperabilità e accountability in un modello più ampio di governance dei sistemi digitali.

Alla base di questo panorama normativo si trova il **Regolamento Generale sulla Protezione dei Dati (GDPR)**, che ha stabilito un riferimento globale per la tutela dei dati personali e la responsabilità delle organizzazioni che li trattano. Il GDPR ha introdotto principi come minimizzazione dei dati, limitazione delle finalità e trasparenza, concetti che oggi influenzano non solo la conformità legale, ma anche la progettazione delle infrastrutture digitali.

Più recentemente, l'**Artificial Intelligence Act** ha esteso questo quadro di governance al dominio dei sistemi algoritmici. Introduce un approccio basato sul rischio in materia di adozione dell'AI, imponendo obblighi specifici ai sistemi considerati ad alto rischio e richiedendo alle organizzazioni di dimostrare trasparenza, tracciabilità e supervisione umana. Poiché l'AI inizia a influenzare i processi decisionali operativi in molti settori, l'infrastruttura che ospita tali sistemi deve supportare meccanismi di monitoraggio, audit e governance.

Accanto a queste iniziative, il **Data Act** mira a rafforzare la portabilità e i diritti di accesso ai dati all'interno dell'ecosistema digitale, riducendo le barriere tra piattaforme e consentendo alle organizzazioni di mantenere un maggiore controllo sui dati che generano. Allo stesso tempo, i framework di cybersecurity come **NIS2** e il **Cyber Resilience Act** introducono obblighi più stringenti per la protezione delle infrastrutture digitali e dei prodotti connessi, mentre **DORA** stabilisce requisiti specifici per la resilienza operativa nel settore finanziario.

Considerate nel loro insieme, queste iniziative mostrano che l'europeicità non è definita solo da dove risiedono i dati, ma dalla capacità delle organizzazioni di dimostrare controllo sulle infrastrutture, sugli standard, sulle supply chain e sui meccanismi di governance da cui dipendono i servizi digitali.

La compliance non può più essere trattata come un requisito a valle: deve essere incorporata direttamente nella progettazione dell'infrastruttura digitale.

Le decisioni infrastrutturali, in merito a dove vengono archiviati i dati, come i sistemi sono interconnessi e quali ambienti ospitano i workload sensibili, determinano in ultima analisi se le organizzazioni possono soddisfare gli obblighi normativi.

L'Intelligenza Artificiale intensifica ulteriormente questa dinamica. I sistemi di AI si basano su pipeline complesse di raccolta, training e deployment dei dati, spesso distribuite su ambienti eterogenei. Garantire la conformità in questi contesti richiede infrastrutture in grado di assicurare tracciabilità, sicurezza e chiarezza giurisdizionale fin dall'inizio. I framework regolatori, quindi, non sono semplici vincoli allo sviluppo tecnologico: sempre più spesso plasmano il modo in cui gli ecosistemi digitali vengono costruiti per rimanere sostenibili e affidabili nel tempo.

Molte organizzazioni stanno ora adottando strategie di sovranità basate sul rischio, concentrandosi innanzitutto sugli strati più sensibili del proprio stack digitale.

Approcci come il **minimum viable sovereignty** riflettono questo cambiamento, incoraggiando le organizzazioni a dare priorità ai controlli nei punti in cui i rischi di governance sono più elevati, tipicamente infrastruttura, governance dei dati e applicazioni critiche, mantenendo al contempo flessibilità operativa altrove.

La qualifica QC3 di Aruba

Un esempio concreto di come il controllo infrastrutturale si traduca in standard operativi è rappresentato dal framework di qualifica definito dall'**Agenzia per la Cybersicurezza Nazionale (ACN)** per i servizi cloud destinati alla Pubblica Amministrazione.

Il framework classifica i dati e i servizi del settore pubblico in tre livelli: **ordinario**, **critico** e **strategico** in base al potenziale impatto che una loro compromissione avrebbe sulla sicurezza nazionale, sulla stabilità economica e sul benessere dei cittadini. I dati strategici includono servizi legati al **Perimetro di Sicurezza Nazionale Cibernetica (PSNC)**, servizi essenziali nazionali regolati dal framework NIS e sistemi che trattano dati altamente sensibili o su larga scala.

I servizi critici, pur essendo meno sensibili di quelli strategici, supportano comunque funzioni pubbliche fondamentali come la sanità o altri servizi locali essenziali.

Per i cloud provider, queste classificazioni si traducono in requisiti tecnici e di governance progressivamente più stringenti. Anche al livello ordinario, i provider devono dimostrare solide garanzie in aree come qualità del servizio, interoperabilità, portabilità e osservabilità.

Man mano che si passa ai livelli critico e strategico, emergono ulteriori obblighi, tra cui localizzazione dei dati all'interno dell'Unione Europea, gestione della cifratura (come il controllo delle chiavi da parte del cliente e l'integrazione di HSM dedicati), capacità avanzate di monitoraggio e processi di validazione della sicurezza più rigorosi.

La resilienza operativa è anch'essa un requisito centrale. Le infrastrutture che supportano servizi critici devono includere

sistemi di backup ridondanti e simulazioni regolari di disaster recovery, mentre gli ambienti strategici introducono ulteriori obblighi relativi alla gestione del ciclo di vita del software, alla sicurezza della supply chain e a procedure formali di reporting verso le autorità.

All'interno di questo framework, la **qualifica QC3 di Aruba** rappresenta il livello più elevato di fiducia per infrastrutture in grado di ospitare i workload più sensibili della Pubblica Amministrazione.

Pur essendo progettata principalmente per garantire la protezione dei dati pubblici strategici, questa qualifica riflette anche la capacità di soddisfare alcuni degli standard più rigorosi in Europa in termini di sicurezza, resilienza e governance.

La qualifica QC3 di Aruba è ulteriormente valorizzata attraverso l'Accordo Quadro Consip, che consente alle amministrazioni pubbliche di accedere direttamente a servizi IaaS e PaaS europei, senza ulteriori

procedure di procurement, accelerando così le iniziative di trasformazione digitale.

Per le imprese che devono orientarsi in contesti regolatori e di sicurezza sempre più complessi, certificazioni come questa rappresentano un punto di riferimento chiaro. Dimostrano che l'infrastruttura europea non è solo un obiettivo politico, ma una capacità operativa concreta che permette alle organizzazioni di combinare conformità normativa, performance tecnologica e resilienza digitale di lungo periodo.

Tuttavia le certificazioni come la QC3 non si limitano quindi ad attestare la conformità ai requisiti del settore pubblico bensì illustrano cosa significa, nella pratica, costruire e governare fondamenta digitali capaci di supportare una sovranità by design, in cui sicurezza, controllo giurisdizionale, resilienza e fiducia operativa sono integrati direttamente nell'infrastruttura.

EVIDENZE DELL'ECOSISTEMA CLOUD EUROPEO DI ARUBA

Qualificazione ACN QC3: Aruba Cloud è qualificata al livello QC3 secondo il framework dell'Agenzia per la Cybersicurezza Nazionale (ACN), il massimo livello previsto per i servizi cloud destinati ai carichi di lavoro strategici della Pubblica Amministrazione. La qualificazione consente inoltre l'accesso ai servizi cloud attraverso gli strumenti di acquisto e gli accordi quadro Consip.

Leadership negli standard aperti: Aruba è membro di Gaia-X e socio fondatore di CISPE. Contribuisce attivamente a iniziative come SECA (Sovereign European Cloud API) e a progetti di infrastruttura aperta quali Liqo e ArubaKube, promuovendo un ecosistema cloud europeo interoperabile, aperto e reversibile.

Modello operativo italiano, sotto normativa italiana ed europea:

Le attività operative di Aruba sono gestite da personale italiano e soggette esclusivamente alla normativa italiana ed europea. Questo approccio riduce l'esposizione a normative extraterritoriali e a richieste di accesso ai dati provenienti da ordinamenti esteri (come il Cloud Act statunitense o altri provvedimenti di discovery internazionale), rafforzando il perimetro di fiducia e controllo per clienti pubblici e privati.

+300.000

SUPERFICIE IN MQ
DEI CAMPUS ITALIANI

80MW

POTENZA IT
DEI CAMPUS ITALIANI

+16MLN

UTENTI

8

DATA CENTER PROPRIETARI
IN EUROPA

evidence box

CAPITOLO 03

Resilienza, interoperabilità e infrastrutture aperte

Se il controllo digitale inizia dall'infrastruttura ed è modellato dai quadri regolatori, la sua efficacia dipende infine dai principi architetturali che guidano la costruzione dei sistemi digitali. Tra questi, resilienza, interoperabilità e apertura sono diventati elementi centrali per garantire che le infrastrutture digitali rimangano adattabili, affidabili e sostenibili nel tempo.

La resilienza è il primo di questi pilastri. Poiché i servizi digitali sostengono sempre più funzioni economiche e pubbliche essenziali, l'infrastruttura deve essere in grado di mantenere la continuità anche in condizioni avverse. Le architetture multi-region, in cui i workload operano su data center distribuiti geograficamente, sono ormai un requisito progettuale fondamentale.

Consentono alle organizzazioni di implementare strategie robuste di disaster recovery, meccanismi di ridondanza e failover operativo, assicurando che i servizi critici rimangano disponibili anche in caso di guasti tecnici o interruzioni esterne.

La sola resilienza, tuttavia, non è sufficiente a garantire controllo strategico e governance del dato. L'interoperabilità è altrettanto essenziale. Negli ultimi dieci anni, molte organizzazioni hanno imparato che affidarsi a un unico ecosistema infrastrutturale può creare dipendenze strutturali che limitano la capacità di adattamento.

Ambienti interoperabili, realizzati sempre più attraverso architetture ibride basate su interfacce standardizzate e API aperte, permettono a workload e dati di muoversi tra infrastrutture diverse senza attriti eccessivi.

Iniziative come **SECA (Sovereign European Cloud API)**, uno standard europeo guidato dall'industria e avviato da provider come Aruba, IONOS e Dynamo per offrire API di gestione cloud aperte, interoperabili e conformi ai quadri normativi UE, favorendo la convergenza EuroStack e l'attuazione del Data Act, e progetti open source come **Liqo** mostrano come layer di orchestrazione standardizzati possano supportare architetture multi provider. Ciò consente alle organizzazioni di combinare servizi hyperscale con infrastrutture regionali mantenendo visibilità e controllo operativi.

In questo contesto, **ArubaKube, il centro di eccellenza di Aruba dedicato alla ricerca, sviluppo e innovazione nelle tecnologie cloud native e nei progetti open source, svolge un ruolo chiave.**

Contribuendo direttamente all'evoluzione di Liqo, ArubaKube promuove un modello pratico basato su open source, interoperabilità e innovazione cloud native, aiutando le organizzazioni a progettare ambienti multi cluster più flessibili, resilienti e pronti per il futuro.

Il controllo non è determinato solo dall'infrastruttura utilizzata direttamente da un'organizzazione, ma anche dagli standard, dalle interfacce, dalle supply chain e dai modelli di governance che collegano provider, piattaforme e partner.

Componibilità e apertura non sono quindi semplici caratteristiche tecniche ma elementi essenziali per ridurre la dipendenza e preservare la libertà strategica nel tempo.

Strettamente legato all'interoperabilità è il ruolo delle tecnologie open source che sono diventate fondamentali negli ambienti cloud moderni, offrendo trasparenza sul

funzionamento dei sistemi e abilitando l'innovazione collaborativa nell'intero ecosistema tecnologico. Per le organizzazioni orientate alla governance di lungo periodo, i framework open source forniscono un ulteriore livello di garanzia: riducono la dipendenza da tecnologie proprietarie e consentono alle infrastrutture di evolvere senza essere vincolate da modelli implementativi opachi.

L'Intelligenza Artificiale rafforza ulteriormente l'importanza di questi principi. I workload AI richiedono una capacità computazionale significativa, in particolare risorse GPU specializzate per attività di training e inferenza. Ospitare questi workload in infrastrutture vicine ai dataset sensibili, e all'interno di contesti giurisdizionali affidabili, diventa sempre più importante man mano che l'AI viene integrata nei sistemi operativi. La disponibilità di capacità computazionale deve quindi essere bilanciata con governance, requisiti di latenza e obblighi di protezione dei dati.

Un altro concetto che sta acquisendo rilevanza nelle strategie infrastrutturali è la **reversibilità architetturale**. Gli ambienti digitali non devono essere solo resilienti e interoperabili: devono anche consentire alle organizzazioni di modificare la propria traiettoria tecnologica nel tempo. La capacità di migrare workload, integrare nuovi provider o adattare i modelli infrastrutturali senza interruzioni strutturali garantisce che le decisioni prese oggi non diventino vincoli domani.

Considerati insieme, resilienza, interoperabilità e apertura costituiscono la spina dorsale operativa di un'infrastruttura digitale europea, consentendo alle organizzazioni di beneficiare dell'innovazione tecnologica globale preservando al contempo la flessibilità, la trasparenza e la governance necessarie per mantenere un'autonomia digitale di lungo periodo.

Aruba: un cloud provider europeo

In questo scenario in evoluzione, il ruolo di Aruba va compreso non semplicemente come quello di un fornitore cloud, ma come un abilitatore infrastrutturale della sovranità per cui essa debba essere incorporata nelle fondamenta degli ambienti digitali fin dall'inizio, attraverso infrastrutture sotto giurisdizione europea, data center resilienti, architetture aperte e interoperabili e modelli di governance allineati ai requisiti di accountability normativa. Questo posizionamento è rafforzato dal ruolo attivo di Aruba negli ecosistemi digitali europei, incluse iniziative come SECA e Gaia X, che contribuiscono allo sviluppo di infrastrutture digitali interoperabili, affidabili e basate su standard.

Questo modello si fonda sulla proprietà diretta e sul controllo operativo dell'infrastruttura sottostante, all'interno di un framework di governance interamente europeo.

In termini pratici, **un approccio sovereign by design non implica la creazione di ambienti isolati. Significa permettere alle organizzazioni di combinare innovazione, compliance, resilienza e controllo di lungo periodo.**

La sovranità non è quindi una funzionalità aggiunta a posteriori, ma una proprietà strutturale del modo in cui l'infrastruttura è concepita, governata ed evoluta. Si basa anche sull'autonomia operativa: la capacità di gestire direttamente infrastrutture, servizi, reti e processi di compliance senza dipendenze strutturali da terze parti.

Sebbene il quadro normativo di riferimento sia definito a livello comunitario, per molte organizzazioni italiane la localizzazione dell'infrastruttura in Italia offre un ulteriore livello di chiarezza e fiducia, in particolare nella Pubblica Amministrazione e nei settori altamente regolamentati, dove semplicità

giurisdizionale, controllo della supply chain e framework di qualificazione locali rimangono elementi chiave.

Questa prossimità giurisdizionale si estende anche al livello umano della gestione infrastrutturale. Il controllo operativo dipende infatti anche da chi gestisce i sistemi: personale soggetto esclusivamente alla legge italiana ed europea garantisce che accountability legale e controllo tecnico rimangano pienamente allineati, colmando così un divario che le sole misure tecniche non possono risolvere.

Per le organizzazioni, tutto ciò si traduce in vantaggi concreti: maggiore controllo sulle scelte infrastrutturali, condizioni di compliance più chiare, portabilità più solida, modelli operativi più prevedibili e un partner in grado di supportare requisiti di localizzazione del dato lungo l'intera supply chain IT.

CAPITOLO 04

Controllo strategico e il paradosso Compute-Compliance

Man mano che l'intelligenza artificiale passa dalla sperimentazione alla piena operatività, le organizzazioni stanno scoprendo che la vera sfida dell'adozione dell'AI non risiede solo negli algoritmi o nei modelli, ma nelle infrastrutture che li supportano. Il passaggio dai proof of concept ai sistemi di produzione solleva questioni più profonde legate a governance, controllo e sostenibilità di lungo periodo. L'AI sta diventando un banco di prova rivelatore delle architetture digitali da cui dipendono sempre più le economie moderne.

Al centro di questa trasformazione c'è il concetto di **controllo strategico (agentività)**. Per imprese e istituzioni pubbliche, la capacità di adottare tecnologie avanzate deve essere accompagnata dalla capacità di governarle/determinare dove risiedono i dati, come evolvono i sistemi e sotto quale giurisdizione operano i workload critici.

L'agentività riflette la capacità di integrare l'innovazione tecnologica globale mantenendo al contempo il controllo sulle condizioni strutturali che la rendono possibile.

Questa sfida emerge con particolare evidenza in quello che può essere definito il **paradosso Compute-Compliance**.

Da un lato, l'Intelligenza Artificiale richiede livelli di capacità computazionale senza precedenti. Addestrare e far funzionare i modelli AI moderni richiede infrastrutture specializzate, connettività ad alte prestazioni e data center sempre più energivori.

Dall'altro, il panorama regolatorio europeo pone un'enfasi crescente su protezione dei dati, cybersecurity, trasparenza algoritmica e accountability operativa.

Se queste due forze evolvono in modo indipendente, le organizzazioni rischiano di trovarsi intrappolate tra imperativi contrastanti: l'accesso a risorse computazionali su larga scala e la necessità di rispettare quadri di governance sempre più stringenti. Risolvere questa tensione richiede infrastrutture capaci di allineare entrambe le dimensioni, offrendo le prestazioni necessarie ai sistemi di Artificial Intelligence avanzati e operando al contempo in ambienti che garantiscano trasparenza, sicurezza e chiarezza giurisdizionale.

È qui che l'infrastruttura digitale europea diventa cruciale. Un'infrastruttura radicata nell'ecosistema europeo può trasformare i requisiti normativi in un principio di progettazione. Integrando compliance, resilienza e governance direttamente nelle architetture digitali, le organizzazioni possono innovare senza perdere il controllo sulla propria traiettoria tecnologica.

Tuttavia l'AI non è solo una svolta tecnologica ma è il primo grande stress test del modello europeo di infrastruttura digitale. Le infrastrutture che supportano l'AI, ovvero data center, architetture cloud, framework di governance dei dati e meccanismi di compliance, determineranno se le organizzazioni potranno sfruttare l'innovazione mantenendo la capacità di plasmare il proprio futuro digitale.

Per molte organizzazioni, costruire un'infrastruttura digitale europea non significherà riprogettare da zero l'intero patrimonio digitale bensì identificare il **set minimo di controlli** necessari per preservare controllo e governance nei livelli più strategici dell'infrastruttura. E quando queste fondamenta vengono stabilite in anticipo, hanno la forza di ridurre l'incertezza di lungo periodo legata a dipendenze tecnologiche, cambiamenti normativi e lock in infrastrutturali, minimizzando la necessità di future repatriation dei workload. La europeicità, in questo senso, non solo mitiga il rischio ma amplia anche lo spazio di manovra, consentendo alle organizzazioni di continuare ad essere competitive in futuro senza essere vincolate da decisioni passate.

In definitiva, controllo e governance non riguardano la limitazione delle scelte tecnologiche ma la costruzione delle fondamenta che preservano la capacità di scegliere e di adattarsi nel tempo. Quando queste fondamenta sono progettate fin dall'inizio attorno a controllo, resilienza, interoperabilità e compliance, riducono l'incertezza e trasformano la localizzazione in Europa del dato in una condizione abilitante per l'innovazione futura.

L'approccio europeo non è un vincolo alla trasformazione, ma una delle sue precondizioni più importanti.

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it