Sistemi distribuiti e trasformazione digitale della PA italiana: dal decentramento operativo a piattaforme nazionali e cloud

Francesco Rombaldoni[1]

[1]f.rombaldoni@campus.uniurb.it

Riassunto

La trasformazione digitale della Pubblica Amministrazione italiana, accelerata dal PNRR, introduce un insieme di infrastrutture e piattaforme nazionali (es. Polo Strategico Nazionale e Piattaforma Digitale Nazionale Dati) che mirano a migliorare interoperabilità, qualità dei servizi e sicurezza. In questa relazione si analizza tale trasformazione anche con lenti tipiche dei sistemi distribuiti: separando la *centralizzazione di governance* (standard, regole, piattaforme abilitanti) dalla *distribuzione tecnica* (cloud, microservizi, federazione, resilienza, replica). Dopo una ricostruzione del contesto pre-PNRR e dei razionali dichiarati dai documenti ufficiali, si propone una discussione critica sui principali trade-off: riduzione della frammentazione e aumento della resilienza, ma anche rischio di concentrazione del valore informativo e dipendenza da processi/competenze operative.
Parole chiave: sistemi distribuiti, interoperabilità, cloud, resilienza, sicurezza, PSN, PDND, PNRR.

1 Introduzione

I sistemi distribuiti sono oggi la forma dominante con cui vengono erogati servizi digitali su larga scala: dai servizi web ai sistemi cloud, fino alle piattaforme che abilitano cooperazione e scambio dati tra organizzazioni. Il corso di *Sistemi Distribuiti* evidenzia come un sistema distribuito non sia solo "più macchine": è un insieme di nodi e servizi che cooperano attraverso la rete, con proprietà desiderabili (scalabilità, disponibilità, resilienza) ma anche limiti strutturali (latenza, guasti parziali, difficoltà di coordinamento, complessità operativa).

Nel caso della Pubblica Amministrazione (PA) italiana, l'interesse per i sistemi distribuiti non è solo tecnologico: la trasformazione in atto riguarda anche *governance, processi, standard* e capacità di realizzare *interoperabilità* in modo sistematico. La documentazione di riferimento (Piano Triennale, documenti PNRR di controllo/gestione, e documentazione PSN) descrive un disegno che combina:

- razionalizzazione infrastrutturale e migrazione al cloud;
- promozione di architetture a microservizi e *API-first*;
- abilitazione del principio *once-only* tramite piattaforme di interoperabilità (PDND);
- rafforzamento dei presidi di cybersicurezza e dei modelli di gestione.

1.1 Obiettivo e struttura della relazione

Questa relazione risponde a tre domande:

1. **Com'era l'infrastruttura e l'ecosistema digitale della PA prima della transizione?**
2. **Che architettura (tecnica e di governance) viene proposta e quali benefici attesi?**
3. **Quali trade-off e criticità emergono in una lettura "da sistemi distribuiti"?**

La parte iniziale è prevalentemente descrittiva, basata sui documenti ufficiali. La parte finale è più critica: non mette in discussione gli obiettivi generali (interoperabilità, qualità, sicurezza), ma discute rischi e condizioni necessarie affinché il disegno funzioni nella pratica.

2 Richiami di teoria: cosa significa "distribuito" (e cosa no)

2.1 Definizioni operative

In letteratura, un sistema distribuito è spesso definito come un insieme di componenti indipendenti che cooperano tramite scambio di messaggi su rete, fornendo all'utente l'illusione di un sistema unico. In tale contesto emergono proprietà chiave:

- **Scalabilità**: capacità di aumentare carico/utenti/nodi senza degradare in modo drastico.
- **Resilienza**: continuità del servizio anche a fronte di guasti parziali.
- **Disponibilità**: probabilità che un servizio sia fruibile in un dato intervallo di tempo.
- **Osservabilità e operabilità**: logging, tracing, metriche, incident response.

2.2 Centralizzazione di governance vs distribuzione tecnica

Nel dibattito pubblico spesso *"centralizzato"* e *"distribuito"* vengono usati come opposti assoluti. In realtà conviene separare due piani:

- **Governance**: standard, regole, contratti di interoperabilità, criteri di sicurezza, cataloghi condivisi, ruoli e responsabilità. Qui può esistere una forte *centralità decisionale/di coordinamento* pur avendo sistemi tecnicamente distribuiti.
- **Tecnologia**: cloud multi-region, replica, microservizi, federazione di identità, edge nodes. Qui il sistema può essere distribuito anche se esistono "poli" o piattaforme nazionali.

La transizione della PA italiana può essere letta come: riduzione della frammentazione mediante strumenti di governance e piattaforme comuni, e contemporanea adozione di infrastrutture cloud (che sono, per natura, sistemi distribuiti).

2.3 Microservizi e interoperabilità

Il Piano Triennale richiama esplicitamente l'adozione di architetture a microservizi, evidenziando benefici come flessibilità, scalabilità, resilienza e integrazione semplificata, ma anche la necessità di *change management* e competenze adeguate [2]. Questo è coerente con l'idea che nei sistemi distribuiti l'organizzazione e i processi sono parte integrante dell'architettura.

3 Il contesto pre-PNRR: frammentazione operativa e interoperabilità ad-hoc

3.1 Ecosistema eterogeneo e autonomia locale

Storicamente molte amministrazioni hanno sviluppato sistemi informativi in modo autonomo, con livelli differenti di maturità, budget, competenze e fornitori. Il risultato è spesso:

- duplicazione di basi dati e procedure simili (es. anagrafiche locali);
- integrazioni punto-punto, spesso basate su accordi bilaterali;
- disomogeneità di protocolli, modelli dati e livelli di sicurezza.

In termini di sistemi distribuiti, questo scenario è *decentrato* nel senso organizzativo, ma non necessariamente "distribuito bene": è un insieme di isole con interconnessioni fragili e non standardizzate.

3.2 Il ruolo del Sistema Pubblico di Connettività (SPC)

Il Piano Triennale ricorda il Sistema Pubblico di Connettività come infrastruttura per l'interscambio e l'interoperabilità tra PA e per l'interconnessione con Internet [2]. Tuttavia, l'evoluzione verso il cloud e verso modelli federati rende necessario ripensare il ruolo di SPC e le sue modalità attuative.

3.3 Problemi tipici di un "distribuito non governato"

Un sistema informativo nazionale frammentato presenta problemi tipici:

- **Guasti e discontinuità**: data center obsoleti e sotto-dimensionati aumentano probabilità di downtime.
- **Sicurezza non uniforme**: posture variabile tra enti; difficoltà di applicare patching, logging e policy omogenee.
- **Integrazione costosa**: ogni nuova interfaccia richiede negoziazioni e implementazioni ad hoc.

I documenti ufficiali richiamano esplicitamente la necessità di razionalizzare e mettere in sicurezza infrastrutture carenti [2].

4 La transizione PNRR: razionalizzazione, cloud-first e piattaforme abilitanti

4.1 PNRR e cornice di gestione e controllo

Il PNRR, oltre a finanziare la trasformazione, introduce logiche di *programma*, cioè obiettivi misurabili (milestone/target), controllo e rendicontazione [3]. Dal punto di vista architetturale, questo impatta indirettamente: impone tempi e priorità (migrazioni, adozione piattaforme), incentivando convergenza verso soluzioni standard.

4.2 Strategia cloud e Polo Strategico Nazionale (PSN)

Il Piano Triennale collega la strategia *cloud-first* alla necessità di migliorare resilienza e sicurezza, ridurre debito tecnologico e costi dei data center obsoleti [2]. In questo contesto, il PSN viene descritto come infrastruttura ad alta affidabilità localizzata sul territorio nazionale, finalizzata alla razionalizzazione e al consolidamento dei CED.

Dal documento sui nuovi servizi PSN emerge una descrizione più tecnica: cataloghi di servizi, modelli (PSN Managed, Secure Public Cloud, Industry Standard), evoluzioni tecnologiche e integrazioni con servizi di sicurezza e governance [1].

4.3 PDND: interoperabilità e paradigma API-first / once-only

La PDND viene presentata come layer focale per la condivisione di e-service e dati, con funzionalità di autenticazione, autorizzazione, logging e governance degli accessi; le PA possono pubblicare API (REST o SOAP per retrocompatibilità) e registrarle in un catalogo [2]. Inoltre sono previsti scenari evolutivi (bulk, asincrono, caching, modelli inversi, delega, open data via API), che richiamano esigenze tipiche di sistemi distribuiti (asincronia, consistenza, caching, streaming/batch).

5 Architettura concettuale del nuovo ecosistema

5.1 Vista a livelli (layer)

Una vista semplificata dell'ecosistema può essere rappresentata come:

1. **Infrastruttura**: cloud (PSN Managed, Secure Public Cloud, altre infrastrutture qualificate), con requisiti di sicurezza, replica, DR.
2. **Piattaforme abilitanti**: identità, pagamenti, notifiche, basi dati nazionali (es. ANPR), strumenti di monitoraggio.
3. **Interoperabilità**: PDND come catalogo e governance delle API/e-service.
4. **Servizi verticali**: servizi degli enti (sanità, tributi, SUAP/SUE, ecc.) progettati con principi di riuso e integrazione.

5.2 Distribuzione tecnica e resilienza

L'adozione del cloud abilita pattern tipici:

- **Replica e failover**: aumento disponibilità tramite ridondanza multi-fault-domain/multi-region.
- **Elasticità**: scalare servizi durante picchi (es. scadenze fiscali).
- **Separazione dei domini**: microservizi con autonomia di deploy e dati (quando correttamente progettati).

Nel documento PSN (parte PSN Managed Oracle Alloy) compaiono concetti di fault domain, region, anti-affinity e servizi di disaster recovery inter-region [1], che sono esattamente strumenti di progettazione di sistemi distribuiti resilienti.

5.3 Governance e standardizzazione

Parallelamente, la governance si rafforza tramite:

- contratti e cataloghi (e-service PDND, cataloghi servizi PSN);
- qualificazione e classificazione (dati/servizi e idoneità infrastrutture);
- linee guida, ruoli (es. RTD) e processi (monitoraggio, sicurezza, change management).

Questa dimensione non rende "centralizzato" il sistema in senso tecnico, ma rende più unitaria la capacità del sistema-paese di comportarsi come ecosistema coerente.

6 Mappatura su concetti di Sistemi Distribuiti

6.1 Fault tolerance e resilienza: guasti parziali come normalità

Nel mondo distribuito bisogna assumere che:

- un nodo può fallire mentre altri restano attivi;
- la rete può introdurre ritardi o partizioni;
- l'operatività dipende da monitoraggio e procedure di recovery.

Il disegno PSN/Cloud Italia enfatizza la necessità di resilienza e continuità operativa, anche attraverso DR e razionalizzazione di data center non adeguati [2].

6.2 Interoperabilità e consistenza: caching, asincrono, bulk

Le evoluzioni previste per PDND includono notifiche asincrone di variazioni, caching locale intelligente, trasferimenti bulk, scambio sincrono/asincrono [2]. Questi elementi si collegano direttamente a:

- **consistenza e cache invalidation** (problema classico: aggiornare cache e repliche);
- **event-driven** e message-based integration (asincrono);
- **batch vs streaming**.

6.3 Microservizi: confini, dipendenze e deployment indipendente

Il Piano Triennale elenca caratteristiche dei microservizi: self-contained, stateless, indipendenza tecnologica e deploy automatico [2]. In termini didattici, questo permette di discutere:

- progettazione di API e contratti (versioning, backward compatibility);
- osservabilità e tracing distribuito;
- gestione degli errori e timeouts (resilienza applicativa).

6.4 CAP theorem (cenno) e scelte pratiche

Anche senza entrare in formalismi, il CAP theorem ricorda che in presenza di partizioni di rete non è possibile massimizzare simultaneamente consistenza e disponibilità. Nella PA, ciò si traduce spesso in scelte pratiche:

- preferire consistenza forte su dati "fonte" (registri primari);
- usare cache/eventi per ridurre carico e latenza su servizi consultivi;
- definire SLA e comportamenti degradati (graceful degradation).

7 Caso di studio: Sogei/AGENAS come esempio di gestione centralizzata di capability distribuite

Nei materiali AGENAS/Sogei emergono elementi tipici di una gestione industrializzata dei servizi ICT: processi ALM, standard ISO, modelli DevOps/Agile, customer care, SOC, IAM,

DR, piattaforme Big Data/NoSQL [3]. Pur non essendo formalmente uno dei tre documenti principali di policy (qui è citato come estratto nel materiale allegato), questo caso è utile per discutere un punto didattico:

Osservazione (taglio da Sistemi Distribuiti)

In un ecosistema distribuito nazionale, non basta che l'architettura "sia cloud": serve una *capacità operativa* (monitoraggio, incident response, change management, DR testato) che è spesso più simile a quella di un grande provider che a quella di un singolo ente locale. La presenza di SOC, IAM e procedure di disaster recovery periodiche è parte della resilienza tanto quanto la replica tecnica dei dati.

8 Discussione critica: trade-off e criticità

Questa sezione raccoglie considerazioni critiche (non necessariamente presenti nei documenti ufficiali) che emergono quando si osserva la transizione come progetto socio-tecnico: infrastruttura + persone + processi.

8.1 Benefici attesi (e perché sono coerenti con i sistemi distribuiti)

- **Riduzione della frammentazione**: più riuso, meno integrazioni bilaterali.
- **Aumento della resilienza**: infrastrutture con fault domain, region, DR e policy di sicurezza più omogenee.
- **Migliore osservabilità**: centralizzazione di log/audit e monitoraggio continuo (se implementati correttamente).
- **Time-to-market**: piattaforme e servizi standard possono accelerare implementazioni locali.

8.2 Rischio di concentrazione: "high-value target"

Un rischio classico dei sistemi che consolidano dati e servizi è la concentrazione del valore informativo: se un attaccante compromette componenti chiave (identità, interconnessioni, cataloghi, piattaforme), l'impatto potenziale cresce.

Questo non significa che "decentrato = sicuro": spesso la frammentazione implica patching scarso e configurazioni deboli. Tuttavia, la centralizzazione di governance rende più *chiaro* quali siano i nodi critici. In termini di threat modeling, la superficie d'attacco può diminuire in ampiezza ma aumentare in valore e in intensità di attacco.

8.3 Fattore umano e processi

Molti incidenti avvengono non per mancanza di tecnologia, ma per:

- errori di configurazione (misconfig), permessi eccessivi, segreti esposti;

- phishing/compromissione credenziali;
- gestione carente del cambiamento (rilasci non controllati, patch non applicate).

In sistemi distribuiti complessi l'errore è inevitabile; ciò che fa la differenza è:

- capacità di rilevare velocemente (monitoring/alerting);
- capacità di contenere (segmentazione, least privilege, incident response);
- capacità di recuperare (backup, DR, esercitazioni).

8.4 Lock-in e dipendenze

La strategia cloud mira anche a mitigare lock-in, ma nella pratica:

- l'adozione di PaaS avanzati accelera sviluppo ma aumenta dipendenze;
- la migrazione di legacy può indurre compromessi (lift-and-shift vs re-architect).

In un'ottica prudente, il punto non è evitare ogni dipendenza (irrealistico), ma governarla: contratti chiari, export dei dati, observability, e competenze interne minime per non perdere controllo operativo.

8.5 Interoperabilità: API come contratto sociale e tecnico

API-first e PDND promettono standardizzazione, ma richiedono disciplina:

- versioning e deprecazione gestiti (backward compatibility);
- qualità dei dati e semantica condivisa;
- auditing e logging coerenti tra enti.

Senza tali elementi, il rischio è replicare il punto-punto in forma "più moderna" ma non realmente interoperabile.

9 Conclusioni

La transizione digitale della PA italiana descritta dai documenti analizzati può essere letta come un tentativo di passare da un ecosistema frammentato e poco standardizzato a un modello più coerente, governato e interoperabile, sostenuto da infrastrutture cloud e piattaforme nazionali.

Da una prospettiva di sistemi distribuiti, emerge un messaggio chiave: non esiste una dicotomia semplice tra centralizzato e distribuito. Il disegno in atto rafforza la centralità della governance (standard, piattaforme, cataloghi) mentre adotta tecnologie intrinsecamente distribuite (cloud, multi-region, microservizi, asincrono). Il successo dipende dalla qualità di implementazione operativa: competenze, processi, osservabilità e sicurezza "by design".

La discussione critica suggerisce che i benefici potenziali (resilienza, qualità, riduzione costi e frammentazione) siano reali, ma richiedano un presidio continuo dei trade-off: concentrazione del rischio, fattore umano, lock-in e complessità di gestione.