LIBRI DI ASTRID

ASTRID

THINK!
The Innovation Knowledge Foundation

Osservatorio sul *cloud computing*
nella pubblica amministrazione

Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità

a cura di
Enrico Acquati, Simona Macellari
e Alessandro Osnaghi

Prefazione di
Franco Bassanini e Roberto Masiero

Passigli Editori

via Chiantigiana 62 – 50012 Bagno a Ripoli (Firenze)
www.passiglieditori.it info@passiglieditori.it

Franco Bassanini* e Roberto masiero**

PREFAZIONE

Il suggerimento alla realizzazione dello studio che qui viene presentato, condotto congiuntamente dalle fondazioni Astrid e THINK!, con la partecipazione di esperti di THINK! e di rappresentanti delle aziende che hanno sostenuto il progetto, nasce da due fattori che, ciascuno con le proprie specificità, sono destinati a rappresentare due momenti di discontinuità rispetto al passato, rispettivamente in ambito politico e tecnologico, con potenziali effetti congiunti di grande rilevanza: le attività legislative rivolte alla trasformazione della pubblica amministrazione per aumentare l'efficienza di questa e dell'intero sistema paese, e la crescente diffusione di nuove modalità d'uso delle tecnologie Ict dovute, tra l'altro, all'affermarsi del paradigma del *cloud computing*; i due temi sono giustamente posti in relazione: è indubbio infatti che l'evoluzione tecnologica può costituire un fattore di supporto e di abilitazione all'evoluzione dello scenario istituzionale, a condizione che il suo utilizzo sia dispiegato secondo linee corrette, introducendo le necessarie modifiche organizzative e funzionali, ponendosi nelle condizioni migliori per sfruttare tutte le opportunità che la tecnologia offre. A questo proposito è utile ricordare come la possibilità e la necessità di integrare servizi e dati (la cosiddetta cooperazione applicativa) erano, da tempo, obiettivi chiari ed evidenti, come lo era la necessità di identificare i presupposti normativi affinché questo potesse avvenire. Le vicende sviluppatesi nel corso degli anni testimoniano, tuttavia, che la maggior parte delle amministrazioni e degli enti, in particolare quelli locali, continuano a gestire ciascuno il proprio sistema informativo senza coordinamento e senza reale integrazione con quello di altre amministrazioni con cui hanno relazioni funzio-

* Presidente della Fondazione Astrid.
** Presidente della Fondazione THINK!.

nali. Il *cloud computing* può ora costituire uno dei fattori abilitanti una visione sistemica e unitaria, grazie alla quale definire le linee architetturali che permettano uno svolgimento integrato ed efficiente delle attività di *back end* e *front end* delle amministrazioni.

In questa situazione sembra allora opportuno porsi in una prospettiva di medio e lungo termine in considerazione da un lato, dello scenario organizzativo e funzionale della pubblica amministrazione centrale e locale verso cui, seppur lentamente, essa sta evolvendo in vista del processo federalista e, dall'altro, del salto tecnologico, qualitativo e quantitativo, che si sta realizzando: il tema del *cloud computing* e delle sue applicazioni nella pubblica amministrazione appare quindi attuale ed affascinante perché, mentre nel Paese si sviluppa la prospettiva di una diversa allocazione dei poteri, delle funzioni amministrative, dei «punti» di erogazione dei servizi pubblici e di gestione delle risorse, proprio l'affermarsi delle nuove tecnologie, o di modalità di gestione della tecnologia come il *cloud computing*, che appaiono evoluzioni irreversibili, suggerisce di definire un modello diverso di approccio alla tecnologia, che sfrutti le possibilità offerte dalla «distribuzione» delle risorse tecnologiche (virtualizzate) e che permetta il ridisegno dei flussi e della distribuzione delle informazioni delle pubbliche amministrazioni, nell'ottica di razionalizzare i processi, e permettere al sistema pubblico di poter interagire in modo più efficiente ed efficace e a costi ridotti con cittadini e imprese.

A questo proposito, nel corso delle attività svolte dall'Osservatorio, è emersa l'utilità di fornire una rappresentazione, ancorché formale, di quanto appena detto: si è pertanto messa a punto una metodologia che permettesse di effettuare l'analisi dei flussi nell'attività di una pubblica amministrazione e, di conseguenza, permettesse di elaborare una visione per processi delle attività medesime su cui basare un approccio applicativo nuovo e più efficiente; si è ritenuto inoltre di utilità applicare tale metodologia al caso di un comune e di una struttura sanitaria di cura al fine di esemplificarne gli utilizzi pratici: l'esito è stato decisamente interessante perché ha permesso di definire dei nuovi approcci applicativi basati sul *cloud computing* per entrambi i casi.

Si è detto dell'opportunità di porsi in una prospettiva di medio e lungo periodo: non si tratta, infatti, di fare proposte per l'immediato, destinate a cadere in un inesorabile dimenticatoio, ma porre all'attenzione di governo e forze politiche temi di rilevanza strategica per lo sviluppo del sistema Paese, individuando esigenze e proposte per il lungo periodo. Il tema ha una sua precipua attualità poiché, mentre nel Paese si dibatte, come detto, su una diversa allocazione di poteri, funzioni amministrative, servizi e risorse secondo un modello di decentramento e di federalismo, proprio l'affermarsi delle tecnologie dei sistemi distribuiti e l'auspicata diffusione pervasiva della banda larga suggeriscono un modello tecnologico diverso che, appunto, comporti la «distribuzione» delle risorse (virtuali), ma la «concentrazione» (che non significa centralizzazione) delle risorse fisiche e reali. Appare quindi inevitabile che, nel medio-lungo periodo, il Paese, ben oltre la tematica della connettività, per altro sempre all'ordine del giorno, abbia la necessità strategica di avere, al servizio degli enti della pubblica amministrazione, ma anche delle aziende, un'infrastruttura Ict fisicamente allocata e gestita sul territorio nazionale che eroghi, secondo il modello *cloud computing*, i servizi infrastrutturali (connettività, *storage* e virtualizzazione), i servizi di piattaforma attinenti la sicurezza, i *data base* e gli ambienti di sviluppo ed infine i servizi applicativi: si tratta di progettare un'infrastruttura a carattere strategico, obiettivo che ha peraltro ampio spazio nella Relazione[1] recentemente pubblicata dal Ministero dello sviluppo economico e che viene richiamata, sia pure in termini generali, dalle recenti iniziative del governo in tema di agenda digitale.

Per arrivare a formulare una proposta di questo tipo è necessario un grande lavoro interdisciplinare che identifichi un percorso pluriennale sia di realizzazione dell'infrastruttura tecnologica del Paese sia di convergenza delle amministrazioni e degli enti verso l'uso dei relativi servizi. È necessario soprattutto un lavoro di analisi preliminare dei servizi utili alle pubbliche amministrazioni ed i vincoli che vi ostano, che consenta di individuare gli interventi normativi necessari per abilitare i cambiamenti conseguenti. Si tratta di un per-

[1] Ministero dello sviluppo economico, *Progetto strategico – Agenda digitale italiana*, Roma, 15 dicembre 2011.

corso lungo e, in un Paese come l'Italia, accidentato e forse visionario: ma non sembra troppo ambizioso ipotizzare che l'evoluzione delle tecnologie Ict possa avere, nel lungo periodo, anche un'influenza positiva sull'architettura complessiva dell'amministrazione di uno Stato del ventunesimo secolo.

Questo lavoro si propone, come detto, di studiare le implicazioni che l'introduzione del *cloud computing*, il nuovo dirompente paradigma di utilizzo delle Ict, potrà avere sulla pubblica amministrazione italiana, anche in relazione al processo di riorganizzazione della architettura della Repubblica in senso federale, e di suggerire le principali azioni necessarie ad abilitarne l'adozione.

È ormai dimostrato, da un gran numero di ricerche e indagini, che il *cloud computing* è un fattore cruciale della crescita economica e della competitività di ogni sistema economico: contribuisce in modo determinate all'incremento della produttività delle imprese, in specie delle Pmi, ed è una grande opportunità per aumentare l'efficienza della pubblica amministrazione; è inoltre un abilitatore della società dell'informazione e della diffusione dell'economia digitale, può generare importanti benefici anche per le famiglie e più in generale per la coesione sociale (si pensi per esempio alle sue applicazioni nel campo dei servizi alle persone e dei sistemi educativi) e, non ultimo, ha forti influenze anche sul comparto delle aziende Ict. Perché possa pienamente dispiegare i suoi effetti positivi per la coesione sociale, la crescita e la competitività del Paese, il *cloud computing* richiede uno sforzo importante nella definizione delle regole, dei comportamenti e delle procedure che devono governare questo nuovo paradigma tecnologico, in modo da accelerarne i benefici e garantire allo stesso tempo la sicurezza degli utenti, delle aziende e del Paese,

Le raccomandazioni di politica strategica, sviluppate nel documento, hanno lo scopo di favorire una discussione aperta e qualificata su come costruire un terreno fertile per lo sviluppo sostenibile del *cloud computing* in Italia: esse si concentrano sui principali destinatari dei servizi del *cloud computing*: le piccole e medie aziende, la pubblica amministrazione in senso lato e il mondo Ict.

Questo studio si concentra sugli aspetti del *cloud computing* che sono rilevanti per la pubblica amministrazione, pertanto appare utile chiarire fin dall'inizio quali sono i potenziali attori di cui si parla: la pubblica amministrazione non è costituita solamente dalle amministrazioni centrali dello Stato, ma da tutti i soggetti attualmente sottoposti alla disciplina del decreto legislativo n. 82/2005 – Codice dell'amministrazione digitale (Cad). Essi sono identificati all'art. 2 – *Finalità e ambito di applicazione* che a sua volta rinvia all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165: «Per Amministrazioni pubbliche s'intendono tutte le Amministrazioni dello Stato, ivi compresi gli istituti e le scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le regioni, le province, i comuni, le comunità montane e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale».

Questa elencazione è ulteriormente ribadita all'art.1 – *Definizioni* del Cad, che al comma 1, lett. *z)*, chiarisce che ovunque nel testo si legga «pubbliche Amministrazioni centrali», la norma si applica alle «Amministrazioni dello Stato, ivi compresi gli istituti e le scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (Aran), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300».

Un Paese avanzato e con un'architettura istituzionale articolata come quella della Repubblica italiana, non dissimile peraltro da quella di molti altri paesi, organizzata in amministrazioni centrali e enti dello Stato, agenzie, regioni, province e comuni, non può consentire, a maggior ragione nella prospettiva di una evoluzione federale, che il trasferimento di funzioni dallo Stato a regioni ed enti locali determini, per i cittadini e le imprese che operano in aree diverse del territorio, una disparità dei servizi essenziali e dei loro livelli di qualità. Ciò non toglie che sia comunque utile distinguere tra i vari tipi di amministrazioni proprio perché, sfruttando le flessibilità offerte dal *cloud computing*, sia possibile fornire le soluzioni più

adeguate alle diverse situazioni.

L'informatizzazione delle amministrazioni è avvenuta in modo frammentato e localistico, non inquadrato in una visione sistemica nazionale; per questa ragione imprese e cittadini, che hanno necessità di accedere – da luoghi diversi da quelli abitualmente di «residenza» – ai servizi erogati dalla pubblica amministrazione, subiscono frequenti, e anche gravi, disservizi con pesanti costi sociali (situazioni socialmente drammatiche si verificano con frequenza, ad esempio, nella sanità). In mancanza di una strategia di standardizzazione delle funzioni e dei servizi da erogare e, soprattutto, di standardizzazione dei dati utilizzati e scambiati tra loro, i sistemi di *back end* di amministrazioni diverse, ma che concorrono ad un unico procedimento di servizio, non sono in grado di interoperare, per superare così i problemi sopraindicati; è facile profezia ritenere che, procedendo sulla strada attuale, il sistema informativo dell'amministrazione del Paese, attualmente composto da migliaia di sistemi informativi autonomi, ciascuno con proprie basi dati contenenti informazioni replicate ed incongruenti, sia destinato a collassare, costringendo sempre più il cittadino a farsi carico dell'impossibilità delle amministrazioni a comunicare tra loro, con il trasferire fisicamente, con costi personali, le informazioni richieste da una amministrazione all'altra. È altrettanto facile profezia ritenere che un sistema, così complesso come quello della pubblica amministrazione, nelle condizioni descritte sia esposto ad un grave rischio di implosione, dovuto a eccesso di produzione documentale cartacea, sempre più difficilmente gestibile con strumenti «manuali».

A questo proposito va ricordato che le tecnologie per l'integrazione di sistemi distribuiti sono disponibili dalla metà degli anni '90 e sono mature e consolidate da oltre dieci anni: presuppongono comunque l'esistenza di una rete e di adeguati servizi infrastrutturali di supporto. Queste infrastrutture di comunicazione sono state concepite e progettate già nell'ambito del progetto «Rete unitaria della pubblica amministrazione» (Rupa) che risale al 1996: di fatto, tuttavia, l'infrastruttura viene utilizzata solo per fornire servizi di accesso ad internet alle pubbliche amministrazioni centrali e è stata aperta alle amministrazioni locali solo successivamente, nell'ambito della evoluzione della Rupa nel Sistema pubblico di connettività (Spc) e nel Sistema pubblico di cooperazione applicativa (Spcoop).

Nonostante gli interventi abilitanti compiuti sul piano normativo a partire dal d.p.r. 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* e, successivamente, dal d.lgs. n. 82/2005 (Cad, integrato recentemente con il nuovo Cad), e nonostante la effettiva realizzazione della Rupa e successivamente del Spc e del Spcoop, l'obiettivo di realizzare l'integrazione dei sistemi informativi delle amministrazioni procedenti con quelli delle amministrazioni certificanti non è mai stato raggiunto. Confrontando i tempi epocali necessari alle amministrazioni per realizzare progetti informatici, con i tempi, rapidissimi, dell'evoluzione tecnologica, si può considerare che il sogno della cooperazione applicativa sia un progetto fallito per scadenza dei termini: oggi infatti si contano sulla punta delle dita i servizi esposti su Spc dalle amministrazioni ed effettivamente utilizzati.

È vero che le amministrazioni possono comunicare tra loro con la posta elettronica, anche quella certificata nelle sue varie forme, ma questo tipo di comunicazione avviene tra operatori e non tra sistemi: è indubbio che cittadini e imprese possono utilizzare servizi *online*, ma i servizi erogati dalle singole amministrazioni hanno un limitato valore economico se i loro sistemi informativi di *back end* non sono direttamente interconnessi con quelli di altre amministrazioni: essi infatti non sono in grado di rispondere in modo integrato alle esigenze di cittadini e imprese, costringendo questi, come già detto, a sostituirsi alle amministrazioni per le fasi a minor «valore aggiunto», come il trasporto dei documenti, comunque dispendiose in termini di tempo. Il cittadino digitale di oggi difficilmente si spiega le ragioni di questa situazione: giova ricordare che l'obiettivo del piano di e-government del 2000 era evitare che, per ottenere un servizio da una amministrazione, il cittadino dovesse fornire documenti ed informazioni già in possesso di un'altra amministrazione: altri 10 anni trascorsi inutilmente! Per questi motivi può essere fatta un'amara considerazione: allo stato attuale il sistema informativo pubblico del Paese, considerato come somma dei sistemi informativi e dalle basi dati operazionali delle diverse amministrazioni centrali e locali, non solo non è un sistema integrato e governato ma non è neppure definibile un sistema!

Vi è infine un aspetto nuovo e di estrema rilevanza da valutare, che rende non più dilazionabile la necessità di assumere delle decisioni d'importanza vitale per il Paese: la sua competitività e la sua sicurezza dipendono da molte infrastrutture strategiche essenziali per il funzionamento di una società moderna: oleodotti, gasdotti, elettrodotti, ferrovie, sistemi di telecomunicazione, poste, ecc. ma a ben vedere tutte queste infrastrutture, gestite da aziende pubbliche o private, dipendono a loro volta dalle proprie infrastrutture Ict, che nei casi citati assumono dimensioni rilevanti, vitali per l'espletamento delle rispettive funzioni operative, e rappresentano anch'esse un patrimonio nazionale. La necessità di un'infrastruttura Ict a carattere strategico-nazionale, che si basi sulle tecnologie e sui modelli proposti dal *cloud computing,* si impone oggi con forza, proprio in relazione ad una evoluzione in senso federale dello stato, non solo per l'esigenza di ottenere i benefici economici attesi dalla evoluzione tecnologica e per la possibilità di razionalizzare e consolidare i sistemi informativi della pubblica amministrazione, ma anche per garantire la sicurezza strategica del paese e la sua competitività.

Nel modello *cloud computing* nelle sue diverse declinazioni, che saranno proposte nel seguito dello studio, i dati non ricadono nel perimetro di sicurezza dell'ente utente ed inoltre la catena dei soggetti che contribuiscono all'erogazione del servizio *cloud* si può estendere anche a livello internazionale, rendendo difficile o impossibile la localizzazione dei dati: un rapporto contrattuale che apparentemente coinvolge solo tre soggetti (l'amministrazione utente, l'*internet service provider* – Isp, e il fornitore del servizio *cloud*), può in realtà coinvolgere una catena difficilmente tracciabile di erogatori di servizi *cloud* e di Isp.

In questo contesto gli utenti di servizi *cloud*, nel quadro normativo vigente italiano ed europeo, restano titolari dei dati, con le conseguenti responsabilità civili e penali, anche quando intervengono soggetti terzi su cui non hanno alcun controllo; è emerso quindi necessario introdurre, a loro tutela e garanzia, un processo di certificazione dei *provider* di servizi ed in particolare dei *cloud provider* che garantisca gli utenti rispetto alle esigenze di sicurezza, di *privacy*, di accordi sui livelli di servizio, sulla localizzazione dei dati e sulle garanzie di portabilità: esso dovrebbe basarsi su clausole contrattuali

standard[2], accertando l'affidabilità del *provider* e di quant'altro possa assicurare la conformità del suo operato alla regolamentazione vigente, nazionale ed europea, sulla sicurezza e sulla tutela della *privacy*; ciò dovrebbe valere anche quando si trattasse di servizi *cloud* eventualmente erogati da amministrazioni ad altre amministrazioni. L'insieme dei fornitori di servizi *cloud* e dei fornitori di servizi internet, che saranno certificati in base alla normativa e ai regolamenti tecnici italiani (da predisporre anche tenendo conto di eventuali analoghe iniziative in sede europea) costituisce di fatto quella nuova infrastruttura strategica Ict che dovrà essere necessariamente considerata tra le infrastrutture critiche del Paese e nel testo definita «Nuvola pubblica certificata» (Npc): essa dovrà essere realizzata e governata con le modalità e gli strumenti che vengono approfonditi e proposti nel seguito dello studio. Questa infrastruttura Ict certificata non sarà funzionale alle sole esigenze dalla pubblica amministrazione, ma potrà offrire servizi anche alle imprese, grandi, medie e piccole che siano, soggette, come le amministrazioni, alla normativa sulla sicurezza e sulla tutela dei dati personali.

La pubblica amministrazione italiana, a livello centrale e locale, dispone di numerose decine di *data center*, alcuni gestiti ancora con tecniche e procedure obsolete, quindi necessariamente costosi e poco efficienti. Una strategia di migrazione verso il *cloud* rappresenta anche un'occasione per rivedere la situazione esistente, con l'obiettivo di razionalizzare, consolidare e modernizzare i sistemi informativi, invece di procedere a costosi investimenti al solo fine di fare fronte al processo di obsolescenza delle dotazioni tecnologiche, senza apprezzabili vantaggi sul piano applicativo e funzionale. Il processo di migrazione verso il *cloud computing* da parte delle amministrazioni dovrà essere necessariamente graduale e si svolgerà secondo diversi modelli architetturali, mantenendo tuttavia integrazione e compatibilità con i servizi esistenti: le strategie seguite potranno essere rivolte all'uso di servizi di *cloud* pubblici, oppure al consolidamento dei propri *data center* in *cloud* privati o di comunità. Per

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:-0005:0018:EN:PDF.

governare la transizione, sono necessari un censimento dei *data center* attualmente operativi, una pianificazione accurata, che includa una *roadmap* di transizione, un prospetto di costi e benefici economici e funzionali e – se possibili – incentivi per favorire l'aggregazione dei *data center* esistenti; nel caso in cui i *data center* appartengano ad enti locali che svolgono gli stessi compiti istituzionali ed erogano gli stessi servizi, si dovrebbe incentivarne la standardizzazione per favorire un consolidamento anche a livello applicativo. Nel censimento dovrebbero rientrare anche i *data center* dei grandi enti pubblici e delle grandi imprese a partecipazione pubblica nazionale e locale spesso dotati di grandi capacità e potenza, superiori a quelle effettivamente utilizzate, ed inoltre espandibili. Come già osservato tutte le infrastrutture critiche nazionali (gasdotti, oleodotti, elettrodotti, ferrovie, autostrade, poste, telecomunicazioni ecc.) sono oggi totalmente dipendenti dalle tecnologie Ict; è presumibile che i soggetti che le gestiscono possiedano *data center* capaci di evolvere, nel quadro di una *partnership* pubblico-privata ben costruita, verso l'offerta di servizi *cloud*, realizzando così l'infrastruttura critica nazionale per eccellenza: una infrastruttura Ict strategica del Paese aperta a tutti nel quadro di un progetto pluriennale.

Vi è un ultimo punto da sottolineare e che ha un ruolo abilitante per eccellenza: le infrastrutture di comunicazione. Il *cloud* pubblico, cioè la modalità di erogazione di servizi più confacente proprio alle amministrazioni e alle piccole e medie imprese, implica che i servizi siano erogati attraverso internet e richiede che i fornitori di servizi di connettività siano in grado di garantire livelli di servizio sufficientemente elevati. L'infrastruttura internet di un Paese, la banda disponibile a imprese, amministrazioni e famiglie, sono il principale fattore abilitante della società dell'informazione e della diffusione dell'economia digitale e sono un prerequisito necessario e indispensabile per l'evoluzione verso il *cloud computing*. Si ripropone quindi il tema della larga banda (*broadband* e *ultra-broadband*) come fattore determinante ed abilitante lo sviluppo del Paese: le caratteristiche della banda necessaria dipendono evidentemente dai modelli di servizio e dalle situazioni applicative, ma in ogni caso occorre fare riferimento ad una larghezza di banda da 20 a 100 Mbps e oltre, tenendo conto delle attuali evoluzioni verso l'ordine di grandezza dei Gbps.

È utile ribadire che i servizi di connettività internet sono un prerequisito necessario per la diffusione di questo nuovo paradigma tecnologico che comporta, come già detto, significativi vantaggi economici; si tratta in primo luogo di garantire universalità di accesso e qualità della rete: la disponibilità diffusa sul territorio di banda larga deve essere orientata prioritariamente alle amministrazioni locali e alle piccole e medie aziende, allo scopo di consentire un uso qualificato di servizi digitali avanzati, che consentano anche alle amministrazioni e alle Pmi italiane di operare in maniera efficace ed essere protagoniste competitive dell'economia globale: senza questo requisito non è ipotizzabile pensare in termini di progetto strategico per il Paese.

RINGRAZIAMENTI

Il rapporto qui presentato costituisce il risultato di una complessa attività di analisi svolta su più fronti: gli aspetti legati allo sviluppo della tecnologia Ict, quelli connessi con l'organizzazione e le funzionalità della pubblica amministrazione, sia centrale sia locale, e quelli relativi ai risvolti istituzionali e legislativi correlati: lo sforzo fatto è stato quello di sviluppare uno schema interpretativo dei fenomeni analizzati, nel senso di cercare di formulare delle ipotesi di soluzione dei vari problemi che vengono posti dall'intreccio dei temi precedentemente accennati.

L'oggetto dell'analisi, e delle riflessioni che sono state condotte, ha quindi carattere multidisciplinare e conseguentemente richiedeva il contributo di esperienze e competenze differenti, che potessero coprire tutti gli aspetti d'interesse: a ciò ha risposto una pluralità di soggetti che, ciascuno con le proprie competenze, hanno permesso la realizzazione dello studio. Tali competenze sono state quelle presenti nelle fondazioni ASTRID e THINK! che hanno promosso la realizzazione dello studio e nelle aziende sponsor che sia lo hanno finanziato sia hanno contribuito allo sviluppo dei suoi contenuti.

L'obiettivo che ci si prefiggeva era forse ambizioso e forse il grado di sviluppo delle tematiche studiate non è risultato omogeneo, ma pensiamo comunque di avere raggiunto un importante obiettivo fornendo ai decisori politici, e non solo a loro, degli utili spunti di riflessione su un tema, il *cloud computing*, che è sicuramente destinato ad avere un ruolo fondamentale nello sviluppo del Paese.

Riteniamo quindi necessario ringraziare le aziende che hanno fornito il loro sostegno per la realizzazione dello studio e precisamente: Accenture S.p.A., Alcatel-Lucent, Cisco Italia, Consip, CSC, Fastweb, HP, IBM Italia, InfoCamere, Microsoft Italia, Oracle Corporation, Telecom Italia; nonché il Garante per la protezione dei dati personali che ha costantemente seguito i lavori dell'Osservatorio. E naturalmente i consulenti e gli esperti di ASTRID e di THINK!, senza il cui impegno lo studio non sarebbe stato possibile.

INTRODUZIONE

Lo studio, condotto congiuntamente dalle Fondazioni ASTRID e THINK! con il sostegno delle aziende sponsor, è principalmente rivolto ai decisori politici ed agli amministratori; nei capitoli che lo compongono affronta le tematiche fondamentali che l'affermarsi, sicuramente irreversibile, del nuovo paradigma tecnologico riassunto nella formula *cloud computing*, pone in particolare alle amministrazioni pubbliche ed alle aziende, soprattutto a quelle medie e piccole, e quindi al sistema Paese. Il *cloud computing* crea una discontinuità nei modelli di utilizzo dell'*information technology* e come tale solleva problemi, fa emergere dubbi ed incontra resistenze: in questo contesto lo studio propone soluzioni organizzative ed operative, che andranno abilitate con opportuni interventi normativi, finalizzate alla realizzazione in Italia di una infrastruttura strategica basata sul *cloud computing*.

Il termine *cloud computing* è oggi largamente diffuso ed è utilizzato spesso impropriamente: ciò non sempre aiuta gli utenti a distinguere alcune soluzioni in uso già da tempo, come le soluzioni di Asp (*application service provisioning*), da quanto di nuovo si propone con il paradigma *cloud*. È quindi utile anticipare, anche se in modo sommario, alcune caratteristiche che saranno approfondite nello studio, e che con precisione definiscono i servizi *cloud* e gli attori che operano in questo nuovo mercato.

Il *cloud computing* è un insieme di servizi che i *cloud service provider* (Csp) erogano agli utenti (*cloud service consumer*) attraverso varie tipologie di rete, in particolare internet, e che possiedono tutti le seguenti caratteristiche, senza le quali si è in presenza di normali servizi *web*:

– la capacità dell'utente di richiedere e gestire il servizio necessario a richiesta, senza necessità di rinnovi o estensioni contrattuali;

– l'accesso ai servizi tramite rete, in modo tendenzialmente indipendente dal tipo di apparecchiatura utilizzato;

– la capacità di gestire e assegnare le risorse di calcolo contemporaneamente a utenti differenti senza decrementi di prestazioni;

– la capacità di gestire dinamicamente e in tempo reale la variabilità dei consumi della domanda di servizio da parte dei singoli utenti;

– la capacità dei provider di misurare andamenti e consumi e di adeguare la risposta al variare della domanda, fornendo il dettagliato dei consumi.

Uno degli aspetti innovativi consiste nel fatto che i servizi *cloud* sono fatturati in base al consumo effettivo di risorse: l'utente non ha necessità di fare investimenti in hardware, spesso sovradimensionati per fare fronte alle esigenze di picco, ed in licenze software, non deve affrontare, prima di essere in grado di avviare una nuova attività, i tempi lunghi di approvvigionamento dei beni di investimento e non ha la necessità di dotarsi di personale capace di gestire direttamente il proprio sistema informatico; questo diventa virtuale, ospitato e gestito nella «nuvola», è necessario acquisire solo connettività internet adeguata e disporre di opportune apparecchiature di accesso (tipicamente un pc o altro). In questo senso i servizi *cloud computing* favoriscono soprattutto l'imprenditorialità nuova e la piccola e media impresa, riducendo l'entità degli investimenti e dei tempi necessari per essere operativi.

Con riferimento ai modelli di distribuzione, si parla di *cloud* pubblico se i servizi sono erogati attraverso internet da soggetti che li vendono sul mercato a disposizione di tutti i potenziali clienti, di *cloud* privato se i servizi sono prodotti e utilizzati da un'unica organizzazione, di *cloud* di comunità se sono servizi destinati ad una specifica categoria di utenti e di *cloud ibrido* se i servizi utilizzati sono composizione di due o più tipi di servizi. Anche i modelli proposti per i servizi *cloud* hanno caratteristiche diverse: nel modello IaaS (*Infrastructure as a service*) si erogano servizi infrastrutturali relativi a capacità elaborativa, di memorizzazione dati, servizi di rete e altri servizi di base come *back-up*, *disaster recovery* e continuità operativa, tutti servizi indipendenti dalle applicazioni dell'utente; nel modello PaaS (*Platform as a service*) sono erogati servizi applicativi di base, quali sistemi operativi, *middleware* e tecnologie di base dati, infine nel modello SaaS (*Software as a service*) vengono erogati servizi di natura applicativa sia di tipo orizzontale (ad esempio servizi di e-mail) che verticali, specifici di un settore applicativo. In virtù di questi servizi, in pratica un'azienda o un'amministrazione può rinunciare del tutto ad acquisire e gestire un sistema informatico reale, sostituendolo con un sistema informatico virtuale e sopportando solo costi correnti invece che costi correnti più costi in conto capitale.

L'erogazione di servizi di *cloud*, in particolare a livello IaaS richiede da parte dei *cloud service provider* la creazione di grandi *data center*, dislocati in diverse località anche di paesi differenti e capaci di ospitare centinaia di migliaia di *server*, e inimmaginabili capacità di *storage*: la loro realizzazione comporta investimenti di alcune centinaia di milioni di euro. Per accedere a servizi *cloud* di questa natura diventa determinante la qualità dei servizi di connettività offerti sul territorio dagli Isp (*internet service provider*). Le caratteristiche della banda necessaria dipendono evidentemente dai modelli di servizio e dalle situazioni applicative, ma in ogni caso si tratta sempre di banda effettiva da 20 a 100 Mbit/s e oltre. I servizi di connettività internet sono quindi un prerequisito necessario per la diffusione di questo nuovo paradigma tecnologico.

La ricerca è focalizzata sulle esigenze della pubblica amministrazione, in particolare su quelle delle piccole amministrazioni ma le problematiche da affrontare sono le stesse che interessano anche le imprese ed in particolare le Pmi; non vengono invece trattati gli aspetti relativi all'evoluzione dei sistemi informativi verso soluzioni di *cloud* privato, che interessano le amministrazioni di grandi dimensioni dotate di importanti data center, e ci si è concentrati sugli aspetti, particolarmente critici, che riguardano l'evoluzione dei sistemi informativi delle piccole amministrazioni verso soluzioni di *cloud* pubblico dove i servizi dei *cloud provider*, come detto, sono accessibili via internet.

La migrazione verso l'utilizzo di servizi *cloud* presenta difficoltà di natura culturale e psicologica, ma anche di natura normativa; le perplessità più rilevanti riguardano la temuta perdita di controllo sui propri dati, che sono trasferiti nella «nuvola»: si tratta quindi di preoccupazioni legate alla sicurezza, alla tutela dei dati personali e alle responsabilità giuridiche che le leggi vigenti attribuiscono ai titolari dei dati. Lo studio offre qualche spunto innovativo su questi

aspetti che richiederà ulteriori approfondimenti. In questo campo il legislatore ha dettato, ancora di recente, principi generali e regolamenti applicabili a tutti indistintamente, che peraltro provengono da una cultura e da un tempo, gli anni '90, in cui non esisteva la rete e non si potevano immaginare le possibilità attuali. Si tratta di prescrizioni riguardanti gli adempimenti di sicurezza, inclusa la tutela della *privacy*, che in futuro sarà opportuno rimodulare per renderle più «sostenibili», accettando ragionevoli margini di rischio e considerando non solo la tipologia del dato, ma anche il suo valore economico: la sicurezza informatica costituisce infatti, per le aziende e le amministrazioni, un costo importante, che tende ad essere indipendente dalla dimensione economica delle aziende e delle amministrazioni; va sottolineato che, in realtà, dal punto di vista della sicurezza e della *privacy*, le soluzioni offerte dai *cloud service provider* sono in generale decisamente superiori a quelle messe in atto direttamente dalle organizzazioni utenti. Il processo legislativo e il consolidamento delle direttive a livello europeo richiederà comunque ancora tempo.

Lo studio ASTRID-THINK! propone una soluzione per consentire, ai potenziali utenti, di utilizzare in tranquillità servizi di *cloud computing* pubblico e, al Paese, di trarne i benefici economici e sistemici prevedibili. Si propone di realizzare in Italia un'infrastruttura Ict strategica, chiamata «Nuvola pubblica certificata», da utilizzare come infrastruttura abilitante per realizzare progetti a valenza sistemica nazionale.

Per quanto riguarda la struttura dello studio si può anticipare che il primo capitolo è a contenuto prevalentemente tecnico e riguarda sia la terminologia che le classificazioni, i modelli dei servizi e le architetture; il secondo sviluppa due importanti casi applicativi: il fascicolo sanitario elettronico e i sistemi informativi dei comuni (soprattutto piccoli e medi). È stato approfondito un modello che consente di valutare i costi di realizzazione e gestione dei servizi al cittadino nel caso ipotetico di utilizzo di soluzioni basate su *cloud computing* e nel caso gli sviluppi procedano in modo convenzionale; il terzo capitolo tratta due argomenti di rilevanza sistemica: il primo è la proposta di realizzare la Nuvola pubblica certificata, il secondo analizza le modalità organizzative per la realizzazione dei progetti

Ict a valenza sistemica nazionale appoggiandosi ai servizi della Nuvola pubblica certificata; il quarto capitolo tratta il tema della riduzione dei costi, degli impatti sul piano occupazionale e sulle relazioni tra lo sviluppo di soluzioni *cloud* e il processo federalista e il decentramento amministrativo, con conseguente ridistribuzione dei compiti istituzionali e amministrativi.

La creazione dell'infrastruttura certificata, descritta in questo studio, presuppone scelte politiche soprattutto attinenti alla catalogazione delle basi dati pubbliche d'interesse strategico per il Paese e, ad esempio, decisioni su quali di esse debbano risiedere in *data center* dislocati sul territorio nazionale; presuppone inoltre interventi normativi abilitanti la creazione ed il governo di tale infrastruttura. Nel modello *cloud computing* i dati delle amministrazioni, ma anche quelli delle aziende, sono sottoposti, nella generalità dei casi, alla normativa italiana ed europea sulla tutela dei dati personali: con l'utilizzo di servizi *cloud* i dati escono fisicamente dal perimetro informatico di sicurezza di diretta responsabilità dell'amministrazione o dell'azienda; la catena dei soggetti che contribuiscono all'erogazione di un servizio *cloud* si estende spesso a livello internazionale, fino a rendere difficile o impossibile la localizzazione dei propri dati: un rapporto contrattuale che apparentemente coinvolge solo tre soggetti – il *cloud consumer* (l'amministrazione o l'azienda utilizzatrice), *l'internet service provider* (Isp) e il fornitore del servizio *cloud* – può in realtà coinvolgere una catena difficilmente tracciabile di erogatori di servizi *cloud*, di *cloud broker* e di Isp che operano in contesti giuridici differenti.

Nel recente documento *Cloud computing: indicazioni sull'utilizzo consapevole dei servizi*[1] il Garante per la tutela dei dati personali propone undici argomentati suggerimenti per gli utilizzatori del *cloud* in tema di verifiche di sicurezza, livelli di servizio, clausole contrattuali e necessità di accertare l'affidabilità del *provider*. È tuttavia facile prevedere che molte piccole e medie aziende avranno difficoltà nell'implementazione di molte tra queste indicazioni, mancando al loro interno delle competenze e risorse necessarie. Ap-

[1] Cfr. www.garanteprivacy.it/garante/document?ID=1819933.

pare quindi opportuno, se non necessario, facilitare le scelte delle amministrazioni e delle aziende introducendo un processo di certificazione dei *provider* che garantisca gli utenti dei servizi *cloud* rispetto alle esigenze di sicurezza, di *privacy*, di livelli di servizio, di localizzazione dei dati e di garanzie di portabilità. A tutela e garanzia degli utenti – che nel quadro normativo vigente restano titolari dei dati, con le conseguenti responsabilità civili e penali, anche quando intervengono soggetti terzi su cui non hanno alcun controllo – il processo di certificazione dovrà essere gestito (sulla base di regolamentazioni da emanare) da soggetti terzi qualificati e indipendenti che possano certificare i *provider* accertando la loro rispondenza a clausole contrattuali di servizio standard e alla regolamentazione nazionale ed europea di sicurezza e di tutela della *privacy*, anche quando si tratti di servizi offerti da pubbliche amministrazioni. Diventa inoltre necessario incaricare altri soggetti terzi professionalmente qualificati per svolgere le funzioni di *auditing*.

La Nuvola pubblica certificata è definita, in termini di architettura concettuale, come: *l'insieme organizzato di fornitori di servizi cloud (Csp) e di fornitori di servizi di connettività internet (Isp) che hanno ottenuto la certificazione di sicurezza e di conformità alla normativa e ai regolamenti tecnici italiani*; così definita la Nuvola pubblica certificata è un'infrastruttura aperta, in quanto i servizi sono accessibili via internet, sia pure utilizzando internet *service provider* certificati (è quindi una *cloud pubblica*), e non pone alcuna restrizione sulla natura giuridica dei *provider*, o relativa al contesto giuridico nel quale i *provider* operano e realizzano i servizi, e neppure sulla natura pubblica o privata degli utenti. Qualora i *service provider* eroghino servizi ad una utenza che opera nel contesto giuridico italiano essi devono garantire di essere stati certificati (anche presso organismi non nazionali) secondo la normativa italiana o eventualmente europea vigente. L'esistenza di questa infrastruttura Ict certificata è funzionale non solo alle esigenze delle pubbliche amministrazioni, ma anche a quelle delle imprese, grandi, medie e piccole, anch'esse soggette alla normativa sulla sicurezza e sul trattamento dei dati personali. Questa impostazione concettuale non impedisce di riservare alcuni servizi *cloud* certificati a particolari categorie di utenti (per esempio ai comuni o alle scuole o anche alle sole pubbliche amministrazioni) realizzando così anche la possibilità di costruire una o più Nuvole di comunità che insistono sulla Nuvola pubblica certificata.

Nel terzo capitolo si affronta il tema dei progetti nazionali a valenza sistemica cioè dei progetti che nascono da obblighi normativi od esigenze che interessano tutte le amministrazioni di un certo tipo, o anche tutte le amministrazioni; sono progetti che, anche a prescindere da esigenze di conformità normativa, hanno lo scopo di evitare che i servizi pubblici erogati ai cittadini siano diversi in funzione del territorio, rispondendo così anche ad una esigenza di coesione sociale. A questo proposito va osservato che oggi le amministrazioni si muovono autonomamente senza azioni e piani coordinati e producono inevitabilmente risultati incompatibili e non integrabili. Un esempio tipico di progetto nazionale a valenza sistemica è un progetto che tenda a dare attuazione, secondo un piano organizzato, agli articoli del Cad 50-*bis* – *Continuità operativa*, e 51 – *Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*: questi articoli prevedono che tutte le amministrazioni realizzino autonomamente funzionalità di *disaster recovery* e di continuità operativa, lasciando l'onere di tutti gli adempimenti previsti sulle singole amministrazioni; realizzare in tempi pianificati queste prescrizioni in modo che, ad una data predefinita e certa, il sistema informatico dell'amministrazione del Paese nella sua totalità possa essere considerato in sicurezza è precisamente quanto si intende per progetto di natura sistemica. Si possono elencare numerosi altri esempi: il fascicolo sanitario elettronico, di cui si discute ampiamente nel secondo capitolo, è un progetto nazionale di natura sistemica perché deve garantire l'unicità del fascicolo sanitario del cittadino, indipendentemente dalla regione dove il cittadino stesso può essere curato. Anche le tematiche cosiddette di circolarità anagrafica si risolvono solo con un progetto di natura sistemica, che coinvolga tutti i comuni nell'esposizione dei propri dati anagrafici alle amministrazioni procedenti. Si deve tuttavia precisare che l'esigenza di implementare e gestire progetti di natura sistemica non ha una necessaria relazione con le tecnologie di *cloud computing*, ma nasce dalla natura integrata delle amministrazioni che collaborano nella realizzazione dei servizi: le tecnologie di *cloud computing* ne sono comun-

que un deciso abilitatore.

La Nuvola pubblica certificata può quindi offrire alle amministrazioni ed alle aziende servizi che consentono di assolvere, più facilmente, ad adempimenti di legge, come nel caso dei servizi di *disaster recovery* e continuità operativa che sono tipici servizi *cloud* IaaS: costruendo questa infrastruttura strategica lo Stato passa da un atteggiamento puramente prescrittivo, che abbandona le amministrazioni a sé stesse, ad un atteggiamento di servizio, in cui mette a disposizione gli strumenti per soddisfare le esigenze di sicurezza del Paese.

L'identificazione, la priorità ed i criteri di finanziamento dei progetti di natura sistemica rientrano nelle responsabilità dei decisori politici ed amministrativi, tuttavia questa tipologia di progetti non è mai stata identificata e realizzata soprattutto per la mancanza di strumenti organizzativi ed operativi adeguati. I progetti di natura sistemica sono molto complessi, perché comportano la gestione dell'azione coordinata di centinaia e, a volte, anche migliaia di amministrazioni autonome: si tratta di gestirli con le moderne tecniche standard di *project management* e di definire, con molta precisione, i compiti e le responsabilità delle istituzioni coinvolte. Le carenze organizzative attuali, che sono evidenziate nello studio per quanto riguarda le responsabilità della definizione degli standard e la gestione progettuale effettiva, portano alla proposta di creare un contenitore tecnico responsabile per questi progetti, i cui compiti e responsabilità vengono analizzati nello studio e possono essere aggregati in vario modo, che comunque confermano la necessità di disporre di una struttura tecnica autonoma e operativa, con le caratteristiche di una Agenzia.

Nel corso delle attività di analisi che hanno condotto alla realizzazione dello studio, alcuni temi sono ricorsi con una certa frequenza; questi sono stati: la riduzione dei costi conseguente l'adozione di soluzioni di *cloud computing*, la riduzione del personale, sempre indotto dall'adozione di soluzioni dello stesso tipo, gli impatti del federalismo sull'organizzazione della pubblica amministrazione locale e centrale e le conseguenti opportunità/problemi correlate all'adozione di soluzioni in *cloud computing*; a questi temi è dedicato il quarto capitolo

Gli esempi studiati, comuni e fascicolo sanitario, hanno dimostrato l'indubbia possibilità di una significativa riduzione dei costi Ict, soprattutto nel medio e lungo periodo: questa riduzione si ha non solo sul fronte dello sviluppo e della manutenzione della soluzione, ma anche su quello della riduzione delle dotazioni hardware degli utenti e dei relativi servizi di gestione e manutenzione; inoltre la logica *cloud* «da uno a molti», cioè la possibilità di fornire la stessa soluzione a una molteplicità di utenti, fa si che vengano abbattuti anche i costi di manutenzione e sviluppo della applicazioni. Lo studio indica anche altri costi certamente riducibili, quali quelli legati al raggiungimento di una maggior efficienza del sistema, di cui però non esistono metriche di misurazione e quindi non sono, al momento, quantificabili, pur essendo significativi.

Il tema del personale è certamente critico: lo studio pone il problema del personale sia degli utenti sia dei fornitori fornendo alcune ipotesi di possibilità di reimpiego del personale eventualmente in esubero; è importante sottolineare che non si è voluto descrivere uno scenario forzatamente ottimistico per evitare di affrontare le criticità che il problema pone: si è solo voluto presentare uno scenario possibile, articolato in tutti i suoi aspetti, rispetto al quale non ci sono fattori ostativi dovuti alla diffusione delle soluzioni in *cloud computing*; certo devono verificarsi alcune condizioni «al contorno», che tuttavia riguardano le caratteristiche e la struttura del settore delle tecnologie Ict in Italia e, probabilmente, anche un differente atteggiamento di forze politiche e amministratori verso l'innovazione: il *cloud computing* è un fattore di profondo mutamento nella direzione della diffusione dell'innovazione, è certamente un fattore di forte discontinuità ed il tema della riduzione del personale che indurrebbe non deve divenire, anche in questa caso, un alibi per rinviarne l'utilizzo e la diffusione.

Più volte, nel corso dei lavori dell'Osservatorio, è emerso il tema del federalismo o, meglio, si è discusso se il federalismo possa influenzare le architetture applicative delle soluzioni tecnologiche quali quelle in *cloud* o, al contrario, se la diffusione delle soluzioni in *cloud computing* passa essere un fattore di supporto all'implementazione del processo federalista; è emerso un aspetto di notevole interesse, in qualche modo centrale rispetto a come il problema

veniva posto: l'evoluzione della architettura istituzionale verso il federalismo infatti, ed il conseguente decentramento amministrativo, richiederanno iniziative di *governance* mirate da un lato a garantire l'interoperabilità dei processi, dei dati e dei servizi tra i livelli centrale, regionale e locale della pubblica amministrazione, dall'altro la necessità di mettere a disposizione soluzioni condivise; questo per evitare che l'autonomia delle regioni e degli enti locali, nella realizzazione di servizi, comporti lo sviluppo di soluzioni funzionalmente e tecnologicamente diverse come risposta a identici requisiti funzionali: in questo modo le soluzioni adottate potrebbero risultare non omogenee e non interoperabili tra loro, con conseguenze difficoltà di gestione, drastica riduzione della loro efficacia e aumento della spesa nel suo complesso: a questi problemi è essenziale faccia fronte una adeguata struttura di *governance*, come delineata sopra.

CAPITOLO PRIMO

DEFINIZIONI E SCENARI TECNOLOGICI

1. Premessa

Dovendo discutere, nel seguito di questo studio, di *cloud computing*, è necessario, sin dall'inizio, eliminare qualsiasi possibilità di equivoco: il *cloud computing* non è una nuova tecnologia, bensì un modo nuovo di rendere disponibile ed utilizzare la tecnologia esistente; meglio ancora si può affermare che il *cloud computing* rende la tecnologia trasparente all'utilizzatore, azienda ente pubblico o privato cittadino che sia, rendendogli disponibili, quando nasce la necessità e a seconda del bisogno, le funzionalità della tecnologia stessa, senza che l'utilizzatore si preoccupi dell'origine di tale funzionalità e delle modalità con cui viene fornita; con ciò si delineano già alcune caratteristiche del *cloud computing*: ubiquità di accesso alle risorse tecnologiche, indipendenza dallo strumento utilizzato dall'utente, immediatezza nella disponibilità e variabilità delle risorse secondo il bisogno. Vi è chi, per sottolineare la discontinuità rispetto alle precedenti modalità d'uso della tecnologia, sostiene il paragone con l'erogazione dell'energia elettrica: come l'utilizzatore di energia elettrica, nel momento in cui «accende la luce», non si preoccupa di chi la stia producendo e di come arrivi sino a lui, così l'utilizzatore di soluzioni *cloud computing* non si domanda da dove arrivi la potenza di calcolo o come arrivi a lui, limitandosi a utilizzarne le funzionalità. Quindi *cloud computing* non come tecnologia ma come nuovo paradigma d'uso della tecnologia, secondo il principio della transizione da possesso ad utilizzo (a pagamento) delle risorse. D'altro canto, nel 2000, J. Rifkin ha scritto: «la proprietà è un'istituzione che si adatta con ritmi troppo lenti alla velocità travolgente della cultura del nanosecondo. Essa si fonda sull'idea che il possesso di un bene materiale per un prolungato periodo di tempo rappresenti, in sé, un valore; che «avere», «possedere», «accumulare» siano concetti positivi. Oggi, però, la rapidità dell'innovazione tecnologica ed il ritmo stordente dell'attività economica mettono in discussione la nozione di possesso. In un mondo di produzioni per-

sonalizzate, di continue innovazioni e aggiornamenti costanti, di prodotti con ciclo di vita sempre più breve, tutto invecchia molto in fretta: in un'economia la cui unica costante è il cambiamento, avere, possedere, accumulare hanno sempre meno senso»[1]. Al di là delle conclusioni cui giunge Rifkin, non si può non riconoscere come alcuni concetti siano sicuramente applicabili anche al caso del *cloud computing*.

Proprio per quanto detto in precedenza, occorre chiarire il paradigma del *cloud computing* nelle sue declinazioni e ciò implica la definizione di alcuni concetti che permettono di identificare in modo univoco e senza ambiguità le sue situazioni d'uso. A tale scopo l'Osservatorio ha messo a punto una serie di definizioni, ricorrendo anche a fonti internazionali, ma «localizzate» rispetto alla pubblica amministrazione italiana: questa attività, preliminare agli approfondimenti successivi condotti nel corso dello studio, è stata seguita dalla definizione dei fattori utili alla descrizione del «modello servizi», successivamente utilizzato per accennare ad alcuni possibili scenari architetturali di servizi *cloud* implementabili per la pubblica amministrazione. Entrambe le attività hanno un carattere propedeutico ma integralmente compreso nello sviluppo dello studio: si vuol dire che non si tratta di una componente che va posta in appendice allo studio, ma di un «vocabolario» preliminare necessario alla comprensione del seguito, in quanto definisce i principi su cui si basa l'erogazione dei servizi in *cloud computing*.

2. Tassonomia e definizioni

2.1. Introduzione

Il *cloud computing* rappresenta una significativa discontinuità nel processo di evoluzione tecnologica e lo si può considerare tale, a maggior ragione, in quanto non è una «nuova» tecnologia o un «nuovo» sviluppo di una tecnologia già disponibile: come anticipato in Premessa il *cloud computing* è un modo nuovo di organizzare e

[1] J. Rifkin, *L'era dell'accesso. La rivoluzione della new economy*, Milano, Mondadori, 2000.

rendere fruibili le tecnologie esistenti, integrandone le componenti e presentando all'utente solo le loro funzioni d'uso; in questa prospettiva le tecnologie non appaiono in primo piano, restando, in certo modo, sullo «sfondo» e assumendo la caratteristica di meri strumenti che abilitano l'attività dell'utente, ma di cui l'utente non percepisce neppure l'esistenza. Forse più scenario a tendere che completamente attuale, è comunque una direzione che ha i tratti dell'irreversibilità.

L'essere di fronte ad un fenomeno nuovo chiede anche approcci differenti dal solito: il primo passo richiede di definire in modo inequivocabile gli «oggetti» di cui si tratterà e le loro caratteristiche, quindi definire il «vocabolario» dei termini che verranno utilizzati; a questo scopo si presentano nel seguito alcune definizioni, tratte dalla letteratura e da esperienze e modelli utilizzati dalle aziende del settore Ict, contestualizzate rispetto agli obiettivi di analisi dell'Osservatorio, allo scopo sia di contribuire alla costruzione di un lessico comune, sia di identificare una serie di spunti e di temi che saranno oggetto di analisi di dettaglio nel seguito dello studio.

A questo scopo verranno discussi:

– il glossario di termini tecnici;

– l'insieme di definizioni basate su modelli standard o su esperienze dirette degli operatori dell'industria o della pubblica amministrazione (Pa);

– le contestualizzazioni di termini e definizioni rispetto a situazioni proprie della Pa italiana;

– le proposte o gli scenari da valutare nel corso successivo dell'analisi.

A seguito delle prime valutazioni, si è rilevato come l'ambito di maggior interesse per approfondire l'analisi sia costituito dalla pubblica amministrazione locale (Pal) ed in particolare dai comuni: allo stato dell'arte, da un punto di vista istituzionale, si può ritenere che la Pal, più della pubblica amministrazioni centrale (Pac), possa trarre benefici dall'adozione mirata e guidata di modelli *cloud based*; indubbiamente gli enti centrali, vuoi anche per le dimensioni e la complessità dei loro sistemi informativi, risultano, in genere, meno predisposti di quelli locali alla fruizione dei benefici del *cloud com-*

puting; un ulteriore elemento suggerisce questa direzione, e precisamente la ripetitività delle funzioni svolte dagli enti locali (tutti i comuni svolgono le stesse funzioni, così come le Aziende Sanitarie) e quindi la possibilità di sfruttare una delle caratteristiche delle soluzioni *cloud based*, cioè la messa a disposizioni nella forma «uno a molti» della stessa applicazione, fatto non possibile nella Pac, ove ogni ente svolge attività applicative sue proprie.

2.2. Glossario

Il glossario che segue fornisce le definizioni raggruppate per aree tematiche secondo la prassi della letteratura in merito.

2.2.1. Caratteristiche essenziali del cloud computing

Si è detto che il *cloud computing* non rappresenta una nuova tecnologia, ma una nuova modalità di organizzare e rendere fruibili componenti tecnologiche già disponibili, focalizzando l'attenzione sulle funzioni d'uso, piuttosto che sugli aspetti meramente tecnologici; ciò costituisce un importante momento di discontinuità che è opportuno sottolineare: vi sono infatti alcune caratteristiche funzionali delle soluzioni in *cloud computing* che le soluzioni tradizionali non hanno, e che lo definiscono in modo inequivocabile; la questione è di fondamentale rilevanza in quanto la mancanza, in una soluzione, di una di queste caratteristiche fa si che la soluzione in questione non possa più dirsi *cloud based*; tali caratteristiche sono:

– *servizio on demand*: è la capacità di richiedere e gestire il servizio contrattualizzato, direttamente e su richiesta, senza necessità di rinnovi o estensioni contrattuali rispetto a quanto definito contrattualmente con il *service provider*;

– *accesso broad network*: è la capacità di accesso ai servizi tramite rete, in modo tendenzialmente indipendente dal tipo di *device* utilizzato, senza la necessità di capacità elaborative locali, di *storage* o applicative;

– *resource pooling*: è la capacità, di erogare e assegnare le risorse parallelamente a utenti differenti, senza decremento delle performance e con capacità di risposta potenzialmente infinita;

– *rapid elasticity*: è la capacità di gestire dinamicamente e in tempo reale la variabilità di volumi e consumi della domanda di servizio dei singoli utenti;

– *servizi misurati*: è la capacità automatica dei *provider* di misurare andamenti e consumi e di adeguare la risposta al variare della domanda, fornendo un dettagliato e puntuale *reporting* all'utente.

2.2.2. Modelli di distribuzione

I servizi *cloud* possono essere distribuiti secondo modelli che caratterizzano l'utente, quali la dimensione e le attività svolte o piuttosto le scelte di tipo economico:

– *cloud privato*: i servizi *cloud* sono utilizzati esclusivamente all'interno di un'unica organizzazione; il sistema di erogazione dei servizi è governato dall'organizzazione stessa ma può essere gestito da fornitori terzi;

– *cloud di comunità*: i servizi *cloud* sono condivisi da numerose e diverse organizzazioni che, a prescindere dalla loro localizzazione territoriale, operano nello stesso contesto giuridico, normativo, regolamentare e contrattuale e che si identificano in una comunità di soggetti che perseguono gli stessi obiettivi operativi e strategici; sono inoltre accumunati dalle stesse esigenze nei confronti dei fornitori di servizi *cloud*, indipendentemente dalla natura dei servizi richiesti (IaaS, Paas, SaaS). Il *cloud* di comunità implica l'esistenza di un soggetto terzo che «governa la comunità». I servizi *cloud* sono tipicamente erogati/gestiti da soggetti esterni alla comunità, selezionati con opportuni criteri; in alcuni casi possono essere erogati/gestiti anche da membri della comunità, purché siano certificati e dispongano delle risorse necessarie;

– *cloud pubblico*: i servizi *cloud* sono erogati attraverso internet da soggetti che li vendono sul mercato, mettendoli a disposizione di tutti i potenziali clienti;

– *cloud ibrido*: è un modello misto in cui il catalogo dei servizi utilizzati da un'organizzazione è determinato dalla composizione di due o più servizi *cloud* (privati, di comunità o pubblici) che rimangono logicamente entità a se stanti, anche se possono essere integrati tra loro.

2.2.3. Modelli di servizi

A prescindere dalla rete su cui sono erogati, i servizi proposti dai *cloud service provider* (Csp) sono comunemente classificati secondo i seguenti modelli:

– *IaaS (Infrastractuture as a service)*: erogazione di servizi infrastrutturali, relativi a capacità elaborativa, *storage*, rete e altri elementi di base, assolutamente indipendenti da servizi applicativi di qualunque tipo;

– *PaaS (Platform as a service)*: erogazione di servizi applicativi di base, come sistemi operativi, *middleware*, linguaggi, tecnologie di base dati; può risultare di particolare interesse per fornire ambienti di sviluppo applicativo;

– *SaaS (Software as a service)*: erogazione di servizi applicativi di qualunque tipo, accessibili indipendentemente dal luogo in cui si trova l'utente e dal tipo di *device* utilizzato;

– *BPaaS (Business – Process as a service)*: evoluzione del SaaS, definisce l'erogazione di servizi non esclusivamente riferiti ad ambiti applicativi ma direttamente alle funzionalità di business o di processo, potenzialmente trasversali rispetto alle piattaforme applicative.

2.2.4. Ruoli degli attori

Il *cloud* prevede l'esistenza di un ecosistema con un numero decisamente vasto di ruoli possibili; quelli indicati di seguito rappresentano un sottoinsieme di tale ecosistema, in quanto vengono considerati quei ruoli che, per loro natura e per contesto di riferimento, possono richiedere una formalizzazione normativa o regolamentare.

I soggetti che operano nell'ambito di architetture *cloud* svolgono i seguenti ruoli:

– *cloud consumer*: è un soggetto fruitore di servizi erogati da uno o più *cloud provider*, con i quali instaura un rapporto contrattuale in qualità di cliente e utente;

– *cloud provider*: è un soggetto giuridico titolare di un insieme di servizi *cloud*, responsabile della loro erogazione ai *cloud consumer*;

– *cloud auditor*: è un soggetto indipendente abilitato in grado di effettuare attività di *auditing*, dei servizi erogati da un *cloud provider*, relativamente alla implementazione e gestione del servizio, alle performance, alla sicurezza, all'aderenza a standard e a vincoli contrattuali o normativi;

– *cloud broker*: è un soggetto giuridico che si pone come intermediario tra *consumer* e *provider*, aggregando diversi servizi *cloud* in uno o più servizi, eventualmente aggiungendo specifiche funzionalità o caratteristiche al servizio; in pratica nei confronti dei *cloud consumer* si comporta come un *cloud provider*;

– *cloud carrier*: i soggetti giuridici che forniscono la connettività tra *consumer* e *provider*, che rende possibile il trasporto dei dati e quindi la loro fruizione.

2.2.5. Reti e servizi

I *cloud provider* possono erogare i loro servizi con diversi modelli di dispiegamento. In funzione della tipologia di rete cui sono connessi i *cloud consumer* si dà origine a *cloud* di diversa tipologia e denominazione: *cloud privato*, *cloud di comunità, cloud pubblico* e *cloud ibrido*. Le tipologie di rete da considerare sono:

– *rete privata*: è una configurazione di rete in cui i *cloud consumer* e i *cloud provider* sono funzioni distinte, nell'ambito di un'unica organizzazione giuridicamente titolare della sicurezza. La rete privata è completamente isolata, tecnologicamente e gestionalmente, e non è accessibile dall'esterno; essa può operare anche in logica «virtuale», garantendo una piena separazione dei dati pur utilizzando segmenti di rete pubblica;

– *rete di comunità*: infrastruttura di rete accessibile solo a specifiche categorie di attori, che rappresentano soggetti giuridicamente distinti, in maniera concorrente per la gestione di traffici differenti, ma comunque isolati, e che mette a fattor comune le infrastrutture, ma non i meccanismi di condivisione dei dati o i protocolli applicativi di comunicazione; i soggetti che svolgono un ruolo di *cloud consumer* appartengono a una comunità in quanto tenuti a soddisfare requisiti comuni di conformità a standard e norme;

– *rete pubblica*: è tipicamente la rete internet, basata su un'unica infrastruttura e un unico protocollo di comunicazione, fruibile e accessibile in maniera condivisa, indipendentemente da esigenze e connotazione degli attori coinvolti.

2.3. Posizionamento degli attori

In considerazione dei riferimenti normativi e di contesto esposti in premessa e successivamente ripresi nel capitolo 4, risulta comunque utile assumere una prospettiva più ampia, ispirata dalle pratiche di mercato più comuni nel settore della pubblica amministrazione. A questo fine è utile considerare quali sono gli attori così come definiti dalla normativa vigente.

La trattazione condotta sino ad ora è stata centrata sugli aspetti a carattere «definitorio» generale, si è cioè voluto, come detto, fornire una sorta di vocabolario comune e di contesto generale, che permetta di proseguire lo sviluppo dell'analisi sulla scorta di concetti noti e condivisi. Occorre ora specificare i soggetti su cui si vuole rivolgere l'attenzione, e che svolgono un ruolo di attori nel mercato che si sta trattando, cioè le amministrazioni pubbliche. Sulla base delle disposizioni riportate nella premessa e nel capitolo 4, tali enti sono:

– ministeri, enti centrali e loro organizzazioni territoriali in Italia e all'estero;

– aziende ed amministrazioni dello stato ad ordinamento autonomo;

– amministrazioni, aziende ed enti del Servizio sanitario nazionale;

– regioni, province, comuni, comunità montane e loro associazioni e consorzi;

– istituzioni universitarie, istituti e scuole di ogni ordine e grado e le istituzioni educative;

– Istituti autonomi case popolari, Camere di commercio, industria, artigianato e agricoltura e loro associazioni;

– tutti gli enti pubblici non economici nazionali, regionali e locali.

Tali attori non esauriscono il contesto di cui ci si occupa, che è invece completato dall'insieme di operatori che con quegli enti, a vario titolo, interagiscono, e precisamente organizzazioni private ed individui quali:

– *provider* di servizi;

– imprese

– liberi professionisti (sia in forma indipendente sia in forma aggregata come ad esempio gli ordini professionali);

– cittadini.

Tutti gli attori potranno usufruire di significativi vantaggi derivanti dall'adozione di servizi *cloud*, naturalmente in modo differenziato rispetto alle proprie caratteristiche ed al proprio ruolo, con riferimento ai seguenti potenziali aspetti:

– *costi*: riduzione degli investimenti, trasformati in costi operativi, ed ottimizzazione dei costi di manutenzione, energia e logistica;

– *flessibilità*: possibilità di cambiare con facilità il proprio portafoglio servizi, in funzione delle esigenze dell'organizzazione, sempre più mutevoli nel tempo;

– *elasticità* e *scalabilità*: possibilità di richiedere facilmente modifiche di carico delle applicazioni (ad esempio picchi di lavoro legati ad eventi, scadenze normative o fiscali) e disporre della necessaria capacità di servizio quando serve (*on demand*), senza necessità di dotarsi di risorse rilevanti, dimensionate sul picco e pertanto di norma largamente sottoutilizzate;

– *costo legato al reale utilizzo*: tramite l'adozione di logiche *pay-per-use* avere la garanzia dell'allineamento naturale della spesa Ict alle reali esigenze operative, evitando il problema di giustificare investimenti per ogni servizio;

– *rapidità di realizzazione di nuove soluzioni*: poter contare sulla disponibilità di servizi già predisposti e a diversi livelli (infrastrutturale, applicativo) consentendo di orientarsi verso logiche di riuso, minimizzando il tempo di realizzazione di nuove soluzioni;

– *ottimizzazione ed interoperabilità dei processi amministrativi/di business*: opportunità di una maggiore standardizzazione e informatizzazione dei processi amministrativi o di business, attraverso l'adozione di strumenti informatici già disponibili ed innovativi, abilitanti l'interoperabilità con altre organizzazioni che fruiscono degli stessi strumenti (ad esempio sistemi di automazione di *workflow* di processi amministrativi e di gestione documentale);

– *razionalizzazione dei processi gestionali e di supporto*: centralizzazione ed automazione delle attività operative e a minor valore aggiunto standardizzazione dei processi/sistemi di *enterprise manage-*

ment (ad esempio i sistemi di gestione delle risorse umane);

– *focalizzazione sul «core business»*: possibilità di focalizzare la spesa e le priorità dell'organizzazione sulle attività *«core»*, demandando a terzi la realizzazione e gestione dei servizi Ict, visti come necessari ma non strategici per l'organizzazione;

– *garanzia della continuità di servizio*: possibilità di fruire delle necessarie infrastrutture per garantire *business continuity* e *disaster recovery*, senza effettuare rilevanti investimenti logistici ed infrastrutturali;

– *miglioramento dei livelli di servizio (Sla)*: l'esternalizzazione a terzi offre maggiori possibilità di definire e monitorare gli Sla dei servizi ottenuti, in quanto legati ad aspetti contrattuali e tipicamente vincolati a logiche incentivanti di *success fee/penalty*, in funzione dei livelli di servizio effettivamente erogati; questo aspetto, al contrario, risulta di particolare difficoltà nel caso di servizi erogati internamente dall'organizzazione stessa;

– *efficienza energetica*: la razionalizzazione e il consolidamento che il *cloud* implica comportano la possibilità di una significativa razionalizzazione dei consumi energetici, facilitando anche l'adozione di *green technologies*;

– *controllo, misurazione e attribuzione dei costi*: possibilità di adozione di logiche di contabilizzazione analitico/industriali, rispetto alle attuali di tipo puramente finanziario; ciò può permettere nuove possibilità sul fronte delle attività di controllo di gestione, con la possibilità di inserire valutazioni di efficienza dell'attività amministrativa, oggi non possibili;

– *mobilità del servizio*: la fruibilità del servizio diventa completamente indipendente dall'infrastruttura tecnologica e dalla sua collocazione fisica (in linea di principio è sufficiente una buona connessione di rete e un qualunque strumento capace di accedervi per fruire del servizio).

Le considerazioni precedenti portano a concludere che, in realtà, non si dovrebbe porre il problema del «se» adottare soluzioni di *cloud computing*, ma caso mai del «quando» e del «come»: il tema, correttamente posto, riguarda il problema di assumere, in tempi rapidi, la decisione di definire una propria strategia e operare le proprie scelte di posizionamento in base al giusto bilanciamento tra ruolo desiderato, investimenti necessari, disponibilità di *asset*, miglioramento della gestione o fruizione dei servizi It, benefici economici relativi all'ottimizzazione della spesa Ict e, più in generale, di maggiore efficienza delle proprie attività.

Con l'affermarsi sul mercato del modello *cloud*, ogni singolo attore dovrà definire progressivamente la propria strategia in funzione degli specifici obiettivi; a questo proposito è possibile identificare i principali criteri che possono guidare la previsione di posizionamento degli attori rispetto ai ruoli ricoperti. Si menzionano alcuni dei principali a titolo esemplificativo:

1. dimensioni: le organizzazioni di grandi dimensioni e/o con una spesa più elevata, avendone la possibilità, tenderanno a mantenere autonomia nella realizzazione e gestione dei servizi Ict, mentre le piccole organizzazioni (e ovviamente gli individui) saranno maggiormente attratte dall'opportunità di demandare a terzi gli oneri conseguenti, puntando su economicità, flessibilità e semplicità di gestione;

2. missione: il ruolo istituzionale delle amministrazioni pubbliche e delle aziende, pubbliche o private, guiderà tali attori nel naturale posizionamento nel mercato *cloud*; a titolo di esempio, gli attori che vedono l'Ict come un servizio necessario ma non strategico saranno maggiormente attratti dall'opportunità di diventare *cloud consumer*;

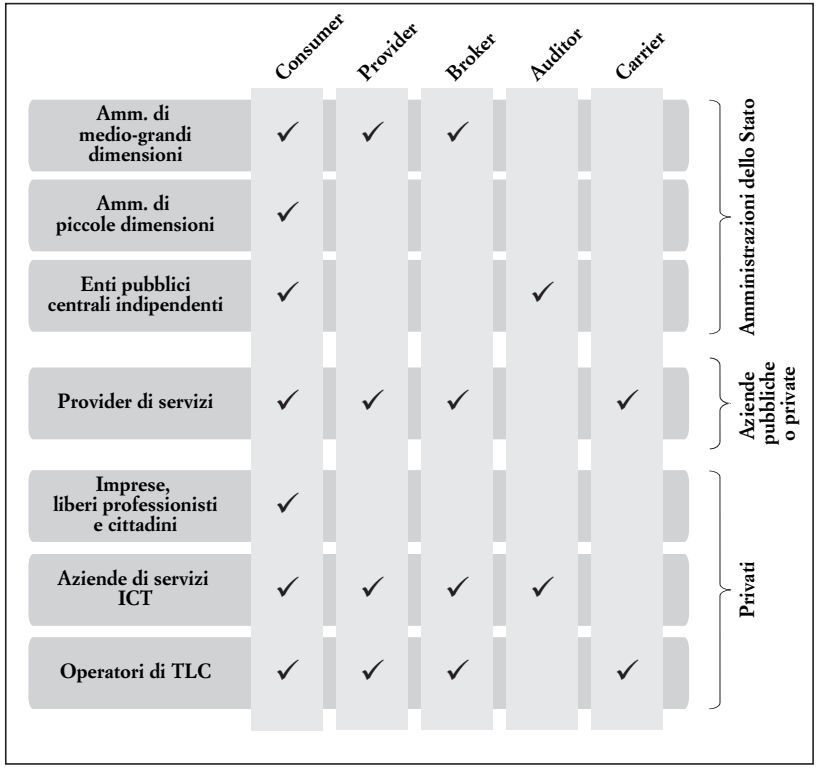
3. asset e competenze Ict disponibili: le amministrazioni o aziende che hanno, oggi, un significativo patrimonio tecnologico (potenza elaborativa, applicazioni, dati, rete) e competenze Ict, tenderanno a conservarle ed a farle evolvere in quanto considerate maggiormente rilevanti per il core business, limitando l'adozione di servizi *cloud* a servizi di «*commodity*» (posta elettronica o simili);

4. mercato o ruolo potenziale: il modello del *cloud* rende possibile l'evoluzione della missione di un'amministrazione o di un'azienda verso modelli nuovi che possono essere attrattivi sia per ragioni di mercato (aziende e provider di servizi) sia di natura politica e organizzativa (creazione di aggregazioni di enti omogenei o sostituzione delle logiche di fornitura).

2.3.1. Ruoli del cloud *e attori della Pa*

In funzione dei *driver* e dei criteri sopra illustrati, è possibile immaginare e definire una matrice di posizionamento illustrata nella figura seguente:

Figura 1. Matrice di posizionamento attori/ruoli



In particolare:

– alcuni enti della Pac e della Pal di grandi dimensioni (ministeri, grandi comuni, province e regioni) tenderanno a trasformare gli asset Ict esistenti e a dirigere gli ulteriori investimenti It verso la costruzione di *cloud* privati o di comunità, con la possibilità di svolgere così un anche ruolo di provider o di *broker* nell'erogazione di servizi It ad altri enti locali; allo stesso tempo potranno essere *consumer* di servizi *cloud* pubblici, dando vita a modelli di dispiegamento tipicamente ibridi;

– gli enti della Pal, intendendo i comuni di dimensioni medio-piccole e altre amministrazioni locali minori**,** tenderanno a rinunciare a mantenere *asset* Ict propri, man mano che sul mercato *cloud* pubblico e soprattutto all'interno della comunità della Pa, a livello centrale e locale, si renderà disponibile un'offerta di servizi in linea con le specifiche esigenze, affidabili, aderenti alle normative ed a costi maggiormente convenienti; tali amministrazioni si posizioneranno pertanto sul ruolo di *consumer*;

– i *provider* di servizi, forti della loro offerta, della loro *customer* base e della presenza capillare sul territorio, tenderanno a presentarsi come «*partner*» degli enti pubblici, e quindi a posizionarsi come *provider* o *broker* di servizi *cloud* nei confronti degli enti della pubblica amministrazione centrale e locale;

– le imprese e i liberi professionisti tenderanno a indirizzare la spesa per *asset* informatici verso servizi *cloud* pubblici e di comunità, e soprattutto potranno disporre di un'offerta di servizi *cloud* maggiormente articolata per l'interazione con la pubblica amministrazione, posizionandosi quindi nel ruolo di *consumer*.

Considerazioni specifiche sono opportune per i *carrier*. È indubbio che il ruolo di *carrier* sarà ricoperto dai grandi operatori di telecomunicazioni presenti in Italia; vanno tuttavia fatte alcune precisazioni: i servizi di rete sono uno dei principali fattori abilitanti i servizi in *cloud* purché a banda larga, date proprio le caratteristiche «intrinseche» dei servizi *cloud* stessi, come per altro indicato sopra; è tuttavia noto come lo stato delle reti di telecomunicazione in Italia presenti alcune criticità, come note sono le difficoltà di decollo delle reti di nuova generazione (Ngn): al momento è quindi difficile capire quanto sia possibile delineare un loro definito ruolo di *cloud carrier* (quindi con relazioni di *business* definite, specifici Sla e caratteristiche di sicurezza delle reti) all'interno del modello di adozione del *cloud* della Pa e delle aziende.

In altre parole occorrerà:

– assicurarsi la presenza fisica dei distributori dei servizi di rete sul territorio nazionale;

– assicurarsi che il livello di copertura dell'infrastruttura di rete a banda larga sia prossimo al cento per cento dei potenziali utilizzatori, e nel caso specifico gli enti della pubblica amministrazione;

– effettuare studi di fattibilità sulle infrastrutture in essere al fine di:

– comprenderne e valorizzarne quelle caratteristiche che garantiscono la gestione sicura del traffico su rete pubblica,

– facilitare l'adozione di soluzioni che semplifichino l'estensione della copertura della banda larga, aumentando la capacità di riuso delle infrastrutture attuali;

– una volta assicurata la necessaria copertura di rete in banda larga, si potrà procedere ad una mappatura puntuale tra modelli di *deployment/delivery* e tipologie/capacità di rete necessarie per l'effettiva fruizione dei servizi (un *cloud provider* privato di servizi IaaS/PaaS avrà sicuramente esigenze di rete radicalmente diverse rispetto a un *cloud consumer* di servizi SaaS/BpaaS magari erogati in *cloud* di comunità).

2.3.2. Modelli di dispiegamento per la pubblica amministrazione

A valle delle considerazioni relative al posizionamento degli attori, e con riferimento alle considerazioni svolte in precedenza, è possibile affermare che il modello che principalmente verrà utilizzato per l'adozione di soluzioni in *cloud computing* nella pubblica amministrazione sarà il *cloud* di comunità, per diversi motivi tra cui:

– le pubbliche amministrazioni con lo stesso ruolo istituzionale (ad esempio i comuni o le scuole) hanno l'esigenza di usufruire di sistemi informativi equivalenti dal punto di vista funzionale, specifici per il loro contesto amministrativo; nel modello indicato è possibile mettere a disposizione di più utilizzatori la medesima applicazione a fronte di esigenze comuni (come gestione documentale, automazione dei processi, controllo della spesa, contabilità finanziaria, gestione personale) contrastando così la tendenza attuale alla realizzazione di soluzioni applicative *ad hoc* per ogni contesto specifico;

– gli enti della pubblica amministrazione hanno ciascuno l'obbligo di garantire, per i propri sistemi informativi, la conformità a norme, regole tecniche, linee guida e, in particolare, al Cad (d.lgs. 82/05) e al Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196). La loro applicazione richiede, tuttavia, investimenti e competenze che esulano delle disponibilità di questi soggetti (che nella stragrande maggioranza sono di piccole dimensioni), e pertanto tali norme restano frequentemente disattese; l'utilizzo di soluzioni in *cloud* di comunità permetterebbe di superare tali difficoltà, mettendo direttamente a disposizione, soprattutto delle amministrazioni di minori dimensioni, un catalogo di servizi già strutturati e a un costo decisamente accessibile, in quanto basati sul principio della condivisione tra molti utenti;

– all'interno della pubblica amministrazione esistono soggetti che possiedono *asset* Ict di dimensioni rilevanti, probabilmente sottoutilizzati, e competenze specifiche per la realizzazione e gestione di servizi Ict complessi, rivolti ad una vasta comunità di utenti: l'utilizzo di questi *asset*, in ambiente di *cloud* privato, comporta inevitabilmente un loro sottoutilizzo, mentre in soluzioni di *cloud* di comunità si realizza la possibilità di mettere a disposizione le risorse ad una pluralità di utenti, con costi suddivisi;

– l'evoluzione della architettura istituzionale verso il federalismo, ed il conseguente decentramento amministrativo, richiederanno iniziative di *governance* mirate da un lato a garantire l'interoperabilità dei processi, dei dati e dei servizi tra i livelli centrale, regionale e locale della pubblica amministrazione, dall'altro la necessità di mettere a disposizione soluzioni condivise; questo per evitare che l'autonomia delle regioni e degli enti locali, nella realizzazione di servizi, comporti lo sviluppo di soluzioni funzionalmente e tecnologicamente diverse come risposta alle stesse esigenze funzionali: in questo modo le soluzioni adottate potrebbero risultare non omogenee e non interoperabili tra loro, con conseguenze difficoltà di gestione, drastica riduzione della loro efficacia e aumento della spesa nel suo complesso;

– la tendenza alla riduzione della spesa nella pubblica amministrazione renderà più attrattiva, per le amministrazioni stesse, l'opportunità di usufruire di servizi già predisposti dai *provider* e certificati da enti preposti, con notevoli risparmi di investimenti e di costi di gestione;

– anche se alcune amministrazioni pubbliche stanno adottando, per alcuni servizi di base, soluzioni di *cloud* di comunità, restano

aperte alcune questioni normative specialmente in tema di conservazione dei dati in loro possesso; la «filosofia» del *cloud computing* ha, per sua natura, dimensione internazionale e localizzazione dei dati non controllabile: da questo punto di vista occorre ricordare che, spesso, neppure il *provider* è in grado di conoscere l'allocazione fisica di un dato, con tutte le conseguenze che ciò comporta dal punto di vista dell'applicazione delle norme italiane ed europee; un *cloud* di comunità della pubblica amministrazione italiana potrebbe indirizzare in maniera non ambigua anche questo tipo di problemi.

L'adozione del modello di *cloud* di comunità per la pubblica amministrazione non implica che i *provider*, all'interno di questo modello, siano necessariamente amministrazioni o aziende pubbliche: è anzi naturale che gli stessi soggetti privati che operano sul mercato del *cloud* pubblico ricoprano i ruoli di *provider*, *broker* o *auditor* di un *cloud* di comunità della pubblica amministrazione. Ciò è giustificato in quanto queste attività richiedono grandi investimenti e competenze nel campo Ict, hanno un ruolo esclusivamente strumentale per gli enti della pubblica amministrazione e non rientrano direttamente nei loro compiti istituzionali.

La pubblica amministrazione è però sottoposta a norme che possono determinare per i *cloud provider* requisiti funzionali, di sicurezza e di affidabilità specifici (come ad esempio il requisito che alcune basi dati risiedano nel territorio nazionale): l'adozione del *cloud computing* richiede quindi il riconoscimento a livello normativo del ruolo dei *cloud provider certificati e accreditati* per la pubblica amministrazione, in quanto in grado di soddisfarne i particolari requisiti. Questo approccio comporta la definizione di un schema di collaborazione pubblico-privato e l'attivazione di un progetto strategico di lungo periodo: il progetto dovrà garantire sia, da parte delle amministrazioni interessate, l'adozione pianificata dei servizi specifici offerti dai *cloud provider*, sia che tale adozione avvenga in tempi certi, al fine di garantire ai *provider* il ritorno dell'investimento; il piano dovrà inoltre prevedere incentivi per le amministrazioni che favoriscano l'adozione di servizi *cloud*. Da ultimo va evidenziato che un simile piano richiede evidentemente un soggetto che lo governi e sia responsabile del raggiungimento degli obiettivi.

Data la rilevanza del tema, questo argomento verrà ripreso e discusso più accuratamente in un capitolo seguente.

Il modello di *cloud* di comunità della pubblica amministrazione è in linea inoltre con l'utilizzo sia della leva dell'innovazione tecnologica sia del modello operativo utile a superare aspetti critici dell'attività di *core business* della pubblica amministrazione, quali:

– l'evoluzione dell'interazione tra amministrazioni e cittadino, liberi professionisti ed imprese verso un modello digitale;

– l'uniformità dei processi e delle procedure amministrative, con l'opportunità di re-ingegnerizzazione di processi e servizi in ottica di semplificazione, automazione e smaterializzazione;

– la gestione integrata dell'enorme patrimonio informativo relativo al cittadino e alle imprese, molto spesso disperso in basi dati di diversi piattaforme di diversi enti (ministeri, enti, regioni, comuni…), con conseguente opportunità di semplificazione e di scambio dati.

2.4. Considerazioni conclusive

La trattazione svolta, al di la di fornire un lessico ed un vocabolario di riferimento utile allo svolgimento del resto dello studio su basi non ambigue, ha inoltre permesso di evidenziare alcuni aspetti fondamentali per la definizione di un'architettura *cloud* per la pubblica amministrazione quali le probabili strategie d'uso delle soluzioni *cloud* da parte dei diversi tipi di enti, piuttosto che il modello di dispiegamento che verrà più probabilmente utilizzato nella pubblica amministrazione o ancora la necessità e l'opportunità di definire ruoli, funzioni ed enti che oggi non sono previsti negli ordinamenti. Questi punti saranno approfonditi nel seguito dello studio, con particolare riferimento agli aspetti istituzionali che devono essere modificati o integrati e che lo sviluppo dello studio ha evidenziato come gli snodo strategici nella prospettiva della diffusione del *cloud computing* nella pubblica amministrazione italiana.

3. Modello servizi

3.1. Introduzione

Nel seguito viene presentata, seppur in forma sintetica ma già ordinata e strutturata, un'ipotesi di «modello servizi» erogabili in *cloud* e rivolti a soddisfare esigenze delle pubblica amministrazione, stante l'attuale quadro normativo e istituzionale.

Allo scopo di facilitare l'esposizione, si sono introdotti criteri di classificazione e categorizzazione che non sono direttamente dipendenti dal modello tassonomico precedentemente definito: si è infatti optato per una scelta basata su criteri funzionali di accorpamento e di prioritizzazione delle esigenze, in un'ottica anch'essa funzionale, dei modelli di servizio: la scelta è stata, in qualche modo, obbligata, ma non per questo meno efficace, data l'assenza, al momento attuale, di un quadro di requisiti funzionali e procedurali strutturato relativo alla pubblica amministrazione, al di là di quello che possa essere desunto dalla normativa primaria e dalla regolamentazione vigente (Cad).

Il modello, in questa fase, si presenta pertanto come un'operazione che può apparire astratta in quanto, alla luce delle considerazioni precedenti, non può essere un modello operativo: vuole però costituire un primo insieme di «applicazioni», senza la pretesa dell'esaustività, sviluppato sulla base di esperienze e interpretazioni di mercato, finalizzato ad avviare una riflessione sui criteri di «categorizzazione» e definizione del modello operativo cui tendere; modello che potrà essere integrato, nella sua evoluzione in senso operativo, anche da *good practicies* internazionali e dalla definizione degli specifici requisiti della pubblica amministrazione italiana. Per questi motivi, la trattazione sarà condotta con particolare *focus* sui servizi di base, infrastrutturali (prevalentemente IaaS e in qualche occasione PaaS o SaaS) e sui servizi abilitanti le soluzioni *cloud* (per esempio i servizi di rete).

3.2. Modelli di classificazione

Si è detto che il contesto di riferimento è definito dell'attuale quadro normativo e organizzativo della pubblica amministrazione, non si considerano quindi scenari istituzionali evolutivi, non ancora definiti nelle sedi di competenza; i servizi definiti in questo ambito non devono richiedere modifiche normative o regolamentari, per lo meno a livello di normativa primaria: permane pertanto il vincolo, attualmente esistente, della mancata identificazione dei servizi sistemici a livello paese e, più in generale, della priorità dei servizi in ottica di sistema e di «continuità di servizio», concetti sui quali si tornerà nel seguito; questo vincolo impedisce sia una corretta definizione di una scala di livelli di servizio in termini di caratteristiche dei servizi stessi, sia una loro corretta categorizzazione, che non sia basata esclusivamente su buone prassi o sul buon senso.

Muovendosi in questo perimetro si sono utilizzati due criteri di classificazione e aggregazione, sviluppati:

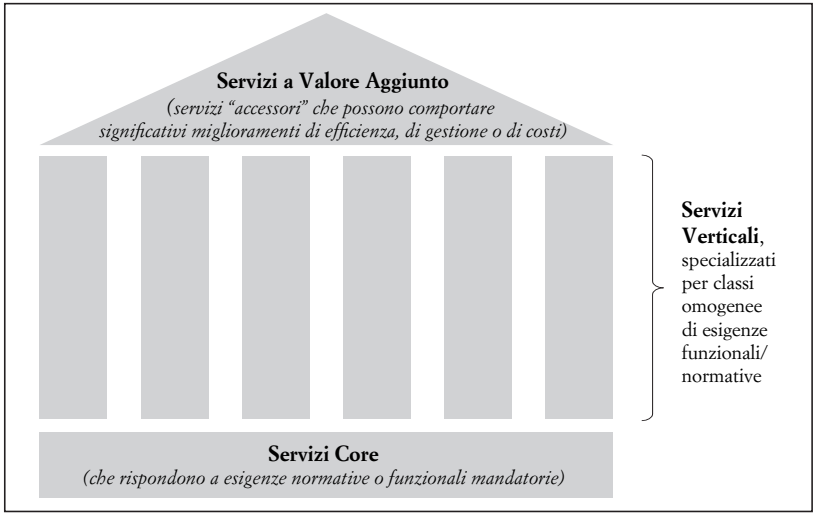
– per esigenze normative e funzionali;
– per classi omogenee architetturali o funzionali.

3.2.1. Modello di categorizzazione per esigenze normative

Questo modello si basa su criteri che permettono di identificare, secondo una logica di classificazione molto elementare, quelle classi di servizio che permettono o facilitano l'adempimento di prescrizioni normative vigenti o di esigenze palesi degli enti della pubblica amministrazione, anche se non formalmente regolamentate.

Il modello può essere rappresentato in questo modo:

Figura 2. Modello di prioritizzazione per esigenze



Questa logica di categorizzazione permette di intercettare con una certa facilità:

– i servizi funzionali a rispondere ad adempimenti obbligatori per tutte le pubbliche amministrazioni, spesso non soddisfatti a causa di difficoltà tecniche o di indisponibilità di *budget* (servizi «*core*»);

– i servizi specializzati per tipi omogenei di enti della pubblica amministrazione, ma rispetto ai quali non è possibile definire della scale di priorità (servizi verticali);

– i servizi, anche non riferiti a specifici segmenti di enti della pubblica amministrazione, ma finalizzati ad aumentare l'efficienza o a semplificare le attività (servizi a valore aggiunto, questi sono tipicamente servizi IaaS, (per esempio servizi di *disaster recovery*) con possibili evoluzioni verso servizi PaaS/SaaS/BPaaS più specializzati (per esempio servizi di *business continuity*).

3.2.2. Modello di categorizzazione per classi omogenee

In questo caso i servizi vengono classificati sotto tre prospettive, non mutualmente esclusive:

– servizi base, auto-consistenti ma fortemente abilitanti l'erogazione di servizi composti, a maggior valore aggiunto o più esplicitamente orientati al soddisfacimento di esigenze normative o operative degli enti della pubblica amministrazione;

– servizi abilitati completamente o in parte dal *cloud* (generalmente servizi *web based*, indirizzati anche al cittadino e non solo agli enti della pubblica amministrazione, in cui il *cloud* può rappresentare l'occasione per una loro effettiva messa a regime, realizzando così anche la standardizzazione di servizi, processi e modelli applicativi); in questo specifico momento, appaiono di particolare interesse per gli enti della pubblica Amministrazione, specialmente locali (es. portale istituzionale o portale del cittadino);

– servizi trasversali rispetto alle modalità di dispiegamento e di *delivery*, ma omogenei rispetto al focus complessivo e funzionali al soddisfacimento di set omogenei di esigenze (es. collaborazione e condivisione informativa e documentale, che possono essere erogati come servizi IaaS e BPaaS).

Questa classificazione non è alternativa alla precedente ma intende integrarla con considerazioni più legate all'offerta di mercato.

3.3. La prima ipotesi di «modello servizi»

3.3.1. Servizi ad alta rilevanza, erogabili esclusivamente in cloud

In questa classe di servizi collochiamo quei servizi definiti come «*core*» nel primo modello di categorizzazione e che possono essere erogati interamente in *cloud*, eventualmente integrando servizi di base auto-consistenti, cioè quelli per i quali la soluzione tecnologica coincide con il servizio finale (*back up* e *recovery*), architetturalmente o funzionalmente omogenei.

3.3.1.1. Servizi di Infrastruttura in *cloud*

Vi rientrano:

– i servizi IaaS funzionali all'acquisizione di capacità elaborativa, *storage*, Tlc e infrastruttura di base di produttività individuale;

– i servizi PaaS funzionali all'erogazione dei servizi precedenti, sistemi operativi, *middleware*, *database*;

– i servizi SaaS funzionali al completamento del servizio di base per la fruizione dell'utente della pubblica amministrazione, per esempio soluzioni *cloud* di *office automation* per la completa implementazione di soluzioni di *virtual desktop*.

3.3.1.2. Servizi aggregati di Infrastruttura in *cloud*

Vi rientrano:

– i servizi IaaS utili alla gestione di funzionalità di *data backup* e *recovery* (Db&r) e di vero e proprio *disaster recovery* (Dr);

– i servizi PaaS funzionali all'erogazione dei servizi precedenti, quali la fornitura, in forma di servizi d'uso, di sistemi operativi, *middleware*, *database*;

– i servizi SaaS/BPaaS funzionali al completamento del servizio di base di *disaster recovery* per la fruizione dell'utente della pubblica amministrazione secondo logiche di classificazione delle funzionalità in una logica standard di *business impact analysis* e di relativa assegnazione delle priorità per il *recovery* (definizione del *recovery time objective* (Rto) e del *recovery point objective* – Rpo);

– i servizi IaaS, PaaS e SaaS funzionali alla gestione dell'identità e

in particolare del *Federated identity management*, intesi come servizi utili/necessari per accedere ai servizi della pubblica amministrazione con credenziali di domini diversi;

– più generalmente, i servizi di sicurezza, trasversali rispetto alle logiche IaaS, PaaS, SaaS e BPaaS, che verranno analizzati successivamente, nell'ambito dei servizi definiti per classi omogenee di esigenze.

3.3.2. Servizi percepiti come ad alta rilevanza dalla pubblica amministrazione abilitati dal cloud

Ci si riferisce qui a quei servizi percepiti come di elevato interesse per la pubblica amministrazione, ma non direttamente qualificati come servizi *cloud* per i quali l'adozione di paradigmi *cloud* può agire come *driver* per l'attivazione degli altri fattori abilitanti, per esempio standardizzazione di funzionalità, di processi o di modelli applicativi.

3.3.2.1. Servizi *web based* abilitati dal *cloud*

Vi rientrano:

– portali istituzionali o rivolti al cittadino, che non rappresentano in quanto tali servizi *cloud*, ma che possono sfruttare l'abilitazione fornita dal *cloud* per facilitare il loro sviluppo e la definizione di modalità comuni di sviluppo e di erogazione;

– strumenti di accesso al mercato, tipo aste *online* o «mercato telematico», per i quali valgono le stesse considerazioni fatte sopra;

– strumenti di gestione patrimoniale e di gestione magazzino, soluzioni *web based* fortemente abilitabili dal *cloud*;

– strumenti di *business intelligence*, Crm e *reporting*, che possono portare un significativo valore aggiunto specialmente nell'ambito degli enti della pubblica amministrazione locale e che possono vedere nel *cloud* privato un fortissimo abilitatore.

3.3.3. Servizi abilitanti i principali servizi cloud

Ci si riferisce qui ai tutti quei servizi, prevalentemente di rete, che rappresentano una «*conditio sine qua non*» o un elemento a valore aggiunto, sia pure auto-consistenti nella loro natura di servizio, funzionale all'erogazione di altri servizi in *cloud*. Si tratta prevalentemente di servizi IaaS legati al mondo delle Tlc.

3.3.3.1. Servizi Tlc *cloud* abilitanti servizi c*loud* aggregati

Vi rientrano:

– i servizi di rete Vpn/Lan specializzati/ottimizzati nel *delivery* di *cloud*;

– i servizi utili a soluzioni di funzionalità di contact center gestito e fornito come servizio;

– i servizi di *security web* e *email*;

– i servizi di *collaboration* e condivisione informativa.

3.3.4. Classi di servizi omogenei per funzionalità erogata

In questo caso ci si riferisce a classi di servizio che aggregano servizi, eterogenei per modello (IaaS, PaaS, SaaS, BPaaS) e per modalità di erogazione, ma omogenei per classe di esigenze indirizzate.

3.3.4.1. *Security* e *business continuity*

Vi rientrano:

– i servizi di *business continuity* già menzionati sopra;

– i servizi di sicurezza logica e perimetrale di tipo IaaS e PaaS;

– i servizi di sicurezza di servizio, *web* o *email*, prevalentemente SaaS, e *office automation*, potenzialmente sia PaaS che SaaS;

– i servizi di sicurezza sui processi, prevalentemente SaaS, in logica di *identity management.*

3.3.4.2. Servizi di pagamento e di controllo di gestione

Vi rientrano:

– i servizi di rete per l'accesso ai canali standard di pagamento interbancario per i pagamenti interni agli enti della pubblica amministrazione, di tipo IaaS e PaaS;

– i servizi di pianificazione e controllo, di tipo SaaS

– i servizi di supporto alla gestione amministrativa in logica di integrazione dei pagamenti – Erp, di tipo SaaS;

– i servizi di interazione Pa – Sistema Bancario a supporto della gestione dei flussi di pagamento verso l'esterno e a supporto della gestione dei fornitori, di tipo SaaS.

3.3.4.3. Condivisione informativa

Vi rientrano:

– i servizi di *digital communication* di base, prevalentemente IaaS;

– i servizi di *messagging* e *instant messaging*, di tipo PaaS e SaaS;

– i servizi di *unified messaging*, fino alla video e tele presenza, di tipo IaaS, PaaS e SaaS;

– i servizi di condivisione documentale, di tipo SaaS;

– i servizi di archiviazione e protocollazione, di tipo IaaS, PaaS e SaaS.

3.3.4.4. Supporto allo sviluppo applicativo e alla gestione del ciclo di vita del software

Vi rientrano:

– i servizi di laboratorio virtuale, funzionale al supporto alla gestione degli sviluppi applicativi, di tipo IaaS e PaaS;

– i servizi di test e *release management* per la gestione dei rilasci applicativi e la loro gestione in logica di ciclo di vita (CdV), di tipo IaaS, PaaS e SaaS;

– i servizi di pianificazione e controllo dei rilasci applicativi, di tipo SaaS.

3.4. Alcune considerazioni

L'approccio adottato, di tipo *bottom up*, ha permesso di definire un «portafoglio» di domanda di servizi *cloud* da parte della pubblica amministrazione e, di conseguenza, di verificare la possibilità, da parte degli operatori di mercato, di erogare tali servizi agli enti della pubblica amministrazione in modo coerente con i riferimenti normativi vigenti.

Nell'ottica di definire il modello operativo, esemplificato successivamente, si può verificare come la percezione delle esigenze delle amministrazioni e delle capacità abilitanti del *cloud* richieda uno sforzo significativo, da parte delle pubblica amministrazione e di chi ne gestisce il quadro di riferimento, in termini regolamentari e funzionali per:

– definire dei criteri di impatto sistemico dei servizi delle pubblica amministrazione che permettano anche un approccio progettuale alla definizione del modello servizi, delle logiche di erogazione e dei relativi impatti operativi, sia in termini industriali che funzionali (esempio tipico quello della sicurezza e della continuità operativa);

– stabilire una prassi standard per la traduzione dei riferimenti normativo-regolamentari in un quadro di riferimenti procedurali e operativi con due obiettivi: da un lato rendere possibile la realizzazione di insiemi standard di specifiche, rivolti agli operatori del mercato e finalizzati alla costruzione di un'offerta coerente con le esigenze della domanda; dall'altro facilitare la definizione di modelli di *business* sostenibili anche e soprattutto per i soggetti privati coinvolti.

3.5. Possibili scenari evolutivi

Più in generale, appare comunque evidente come, l'esigenza di un approccio progettuale dotato di una vista «sistemica» risulti determinante per la costruzione di qualunque modello di servizi supportati da sistemi di automazione, in particolare laddove si vogliano correttamente sfruttare i benefici derivanti dall'applicazione di nuovi paradigmi come il *cloud computing*.

In quest'ottica potrebbe risultare utile sfruttare sinergie con iniziative già in corso, relative alla gestione delle infrastrutture critiche, applicate in contesti complementari e comunque ad alto livello di utilizzo Ict, come quelle delle infrastrutture considerate esplicitamente critiche (d.lgs. 61/2011 che adotta la Direttiva europea 104/2009) quali energia e trasporti o quelle implicitamente critiche controllate da enti regolatori deputati come Banca d'Italia per il settore bancario, cui vengono richieste specifiche priorità di servizio sotto un controllo molto serrato.

3.6 Scenari architetturali

L'applicazione dei modelli sopra descritti ha precisi riferimenti architetturali e tecnologici, che vengono descritti in dettaglio, basati su standard internazionali, nell'Appendice 1: tuttavia quel che appare di maggior rilievo in questa sede è che tale applicazione è non solo possibile ma effettiva. L'esperienza internazionale dimostra che il modello *cloud* permette una flessibilità di soluzioni e di architet-

ture decisamente senza precedenti. Il modello è a livelli successivi, differenti e completamente autonomi, il che permette di intervenire a qualunque livello dell'architettura, senza condizionamenti nell'integrazione derivanti da tecnologie o modelli di sviluppo.

In sintesi, il modello tradizionale che prevede almeno tre livelli, quello infrastrutturale (dalle Tlc alla capacità elaborativa allo *storage*), quello degli ambienti applicativi e di *middleware* e quello dello sviluppo applicativo, vedeva un forte condizionamento di un livello verso gli altri, perché la scelta della piattaforma tecnologica condizionava la scelta degli ambienti applicativi e delle competenze di programmazione.

Il modello *cloud* permette di intervenire sui tre livelli in maniera completamente indipendente, con l'unico prerequisito richiesto che i livelli siano capaci di esporre dei servizi, non in termini tecnici ma funzionali, ai quali gli altri livelli tecnologici possono far riferimento.

Questo significa che la declinazione concreta del *cloud* permette di immaginare soluzioni che vedano:

– l'intera filiera erogata in *cloud*;

– solo uno o più livelli erogati in *cloud* con i restanti erogati in modalità tradizionale, in *house* o in *sourcing*;

– l'erogazione dei servizi in maniera tradizionale con apertura solo di alcune funzionalità a servizi *cloud* pubblici (ad esempio la mail).

In questo scenario, la flessibilità del modello apre, potenzialmente, il mercato con estrema facilità a un ampliamento dell'offerta, anche molto più puntuale e specializzata rispetto ai servizi offerti, semplificando molto il processo di gestione della domanda, che può diventare allo stesso tempo molto più verticale sulle esigenze e molto più standard sulle soluzioni, e abilitando una potenziale razionalizzazione e semplificazione dei costi e del modello di acquisizione.

Il punto di forza rispetto ad altri modelli per servizi è rappresentato dal fatto che i servizi esposti non sono servizi tecnologici, come nei modelli Soa[2] che possono essere un abilitatore del *cloud*, ma servizi funzionali, di processo, rispetto ai quali i *layer* successivi non hanno alcuna dipendenza tecnica.

Si vedrà in seguito come questo possa portare vantaggi significativi in termini di opportunità di efficienza e di riduzione dei costi, oltre che di *procurement*.

[2] *Service oriented architecture*.

Capitolo Secondo

COMUNI E SANITÀ: BENEFICI DELLE SOLUZIONI IN *CLOUD*

1. Premessa

Lo studio, come si è detto, intende fornire un quadro completo delle problematiche legate all'utilizzo di soluzioni in *cloud computing*: a questo proposito si sono definiti una tassonomia e un modello servizi che, se pur indirizzato alle esigenze della pubblica amministrazione, ha comunque caratteristiche di generalità, e nel seguito verranno discusse le tematiche legate al tema della *governance*, aspetto cruciale e di assoluta priorità; si è anche detto che lo studio, pur rivolto a tutta la pubblica amministrazione, centrale e locale, ha un particolare focus sugli enti locali, data la loro maggiore «predisposizione», dal punto di vista strutturale e funzionale, all'utilizzo di soluzioni in *cloud computing*. In questa prospettiva, volendo approfondire l'analisi, si discuteranno due specifici aspetti legati all'utilizzo di soluzioni in *cloud computing*, che hanno valenza generale ma qui applicati a due categorie di enti della pubblica amministrazione locale: comuni ed enti sanitari.

Il primo aspetto di cui ci si occuperà è applicabile a qualunque situazione d'inserimento delle tecnologie Ict in un'organizzazione: ci si riferisce all'analisi delle attività delle organizzazioni secondo la logica dei flussi informativi che le «percorrono» e che conduce nell'analisi funzionale delle organizzazioni a un approccio «per processi», sulla base dei quali vengono disegnate le soluzioni tecnologiche; questo approccio ormai consolidato, secondo quello che viene definito «modello processi/sistemi», in diverse metodologie adottate ormai da decenni nell'industria privata, raramente utilizzato, se non quasi sconosciuto, nella pubblica amministrazione, per lo meno nel passato, diviene di grande attualità e necessità, nel caso di soluzioni *cloud computing*, date la caratteristiche «sistemiche» che queste rivestono. Il secondo aspetto è quello della riduzione della spesa Ict, uno dei temi più interessanti e dibattuti legati all'utilizzo di soluzioni in *cloud computing*: è noto infatti come si ritenga che questo tipo

di soluzioni rendano possibili significative riduzioni di costi, in seguito all'adozione di logiche *pay per use*, alla trasformazione degli investimenti in costi operativi, alla possibilità di ottimizzare i costi di manutenzione, di energia elettrica e di logistica; è altrettanto noto come si ritenga che tali soluzioni inducano anche una serie di risparmi e riduzioni di costi, non di natura Ict, legati alla possibilità di recuperare efficienza operativa nello svolgimento delle attività interessate da soluzioni in *cloud*. Nel seguito verranno sviluppati due modelli, uno con riferimento ai comuni e l'altro agli enti sanitari, volti a fornire indicazioni in merito.

Si cercherà anche di evidenziare come i due aspetti siano in qualche modo correlati in una soluzione in *cloud computing* non tanto dal punto di vista logico-funzionale quanto, piuttosto, da quello temporale, nel senso che il primo, permettendo l'implementazione di soluzioni particolarmente efficienti, induce gli effetti del secondo.

Nel seguito, pertanto, dapprima si delineerà un metodo per definire un modello di analisi che evidenzi l'approccio per processi, successivamente si applicherà tale metodo ai comuni e quindi si effettueranno le stime di spesa di soluzioni *cloud computing*, «derivate» dall'approccio descritto, comparate con la situazione attuale; analogamente si procederà con gli enti sanitari, con particolare riferimento al tema del fascicolo sanitario elettronico (Fse), data la sua particolare rilevanza nei processi connessi alla saluta del cittadino, come illustrato nel seguito.

Un ultimo aspetto, estremamente importante anche per i potenziali riflessi sociali, cioè quello della riduzione del personale che le soluzioni *cloud computing* inducono, verrà discusso alla conclusione del capitolo; il fenomeno è molto controverso, anche perché non esistono, al momento, metriche precise per dirimere il problema: riguarda infatti non solo il personale che opera nei centri Ict e nei processi aziendali degli utenti, grandi o piccoli che siano, ma anche quello delle aziende fornitrici di tecnologia, comunque destinate a modificare il proprio modo di operare e di rapportarsi al mercato: si cercherà pertanto di analizzare il problema nel contesto più ampio, come quello cui si è accennato, al fine di evidenziare tutti i possibili effetti sull'occupazione.

2 Gli strumenti per l'analisi

2.1. Il contesto

Come glia osservato in altra parte dello studio, i progetti d'informatizzazione delle amministrazioni pubbliche, ma non solo questi, sono stati frequentemente condotti, per lo meno in una fase iniziale della diffusione della tecnologia Ict, senza che, preventivamente, venissero definiti ed analizzati i processi che si svolgono nelle amministrazioni stesse e tra le amministrazioni, scegliendo un approccio per «silos» funzionali, sostanzialmente non comunicanti tra loro. Inizialmente si sono informatizzate attività rivolte al funzionamento interno degli enti (bilancio, paghe e stipendi, ecc.), di carattere prevalentemente amministrativo; in genere sono state considerate come attività autonome rispetto al contesto complessivo dell'ente, mentre è noto come queste attività abbiano, in realtà, relazioni continue con le varie unità organizzative dell'ente stesso, e con unità organizzative di altri enti esterni (a questo proposito basta pensare a quanti sono gli enti con cui un'amministrazione pubblica dialoga per la gestione del personale). In una fase successiva il tema dell'informatizzazione è stato affrontato con un'ottica più ampia, considerando l'insieme dei compiti di una singola unità funzionale (le attività di un dipartimento o di una direzione generale), ma sempre come se l'unità funzionale fosse «chiusa» in se stessa, come se esaurisse le proprie attività all'interno dei propri confini.

Le modalità e le logiche con cui, negli scorsi anni, si è introdotta negli enti pubblici la tecnologia, in parte dovute anche a limiti della tecnologia disponibile al momento, hanno portato così alla creazione di «isole», spesso non comunicanti tra loro; negli anni successivi, man mano che la tecnologia ha messo a disposizione nuovi strumenti, si è cercato, a volte anche con successo, di trasformare queste isole in sistemi più organici: non si è tuttavia riusciti a costruire un «sistema integrato», come in realtà è la pubblica amministrazione. La mancata realizzazione di un disegno di questo tipo ha avuto conseguenze rilevanti; basti pensare a tutti gli inutili tentativi di «dematerializzare» le relazioni tra cittadino e pubblica amministrazione, volti a fare sì che le amministrazioni reperissero direttamente le informazioni e i documenti di cui necessitano, quando generati da un'altra amministrazione, senza che i cittadini, ridotti a semplici

«porta carte», siano costretti a fare inutili file agli sportelli: ma per fare ciò sarebbe occorsa una visione complessiva, dotata al tempo stesso di organicità e sintesi, che è invece mancata. Anche recentemente si è assistito alla formulazione di un piano per l'e-government costituito dalla somma di un certo numero di progetti proposti da singole amministrazioni: un approccio *bottom up* come questo non permette di realizzare una visione globale, e soprattutto integrata, dei processi della pubblica amministrazione, e non è certamente quello che serve.

A questo proposito, va tuttavia ribadito che una qualunque unità funzionale di un'amministrazione (centrale o locale, direzione generale, dipartimento o quant'altro) non svolge la propria attività esclusivamente all'interno dei propri confini ma, in misura differente secondo gli obiettivi e le funzioni svolte, può avere interazioni, sia in entrata sia in uscita, con altre unità funzionali della medesima amministrazione o di altre amministrazioni, centrali o locali. In realtà ogni attività è, in generale, «inscrivibile» in un'istanza «maggiore», costituita da altre attività che hanno tra loro relazioni funzionali tali da dare «un senso compiuto» all'insieme delle attività stesse: in altre parole l'istanza «maggiore» di cui si è detto è riconducibile ad un processo; è pertanto possibile affermare che ogni unità funzionale opera per processi o, se si vuole, all'interno di processi, che si svolgono o nella stessa unità funzionale, o all'interno di una determinata amministrazione, o coinvolgono unità funzionali di altre amministrazioni.

Negli scorsi anni, soprattutto nella pubblica amministrazione, il tema dell'analisi dei processi, o meglio per processi, è rimasto sostanzialmente sullo sfondo e la tecnologia ha continuato ad essere fondamentalmente applicata secondo i criteri cui si è accennato in precedenza. Si è quindi assunto il primato della tecnologia, lasciando a lato il tema strategico dell'analisi per processi che, inoltre, avrebbero potuto ricondurre alla ridefinizione, quando non alla revisione e reingegnerizzazione, dei processi stessi. Lo sviluppo e l'evoluzione delle tecnologie mettono attualmente a disposizione soluzioni che richiedono sempre più un approccio «sistemico», basato appunto sull'analisi per processi delle organizzazioni in cui le soluzioni tecnologiche vengono realizzate. Con riferimento al contesto dello studio,

ma anche in via più generale, occorre, a questo proposito, riprendendo per altro considerazioni già fatte, chiarire preliminarmente che il *cloud computing* non è in realtà una nuova tecnologia: è invece un modo nuovo di organizzare e utilizzare le tecnologie disponibili, che integra le componenti puramente tecnologiche presentando all'utente solo i loro aspetti funzionali, realizzando con ciò una discontinuità nel processo di sviluppo delle tecnologie, proprio in quanto queste non svolgono più il ruolo di primo piano che era loro attribuito, ma vengono trasformate in un puro fattore strumentale.

Se si considera in particolare la pubblica amministrazione, è innegabile che un ente (o una sua unità funzionale) può essere considerato una struttura a carattere «sistemico», con differenti livelli di complessità a seconda delle caratteristiche e delle attività svolte: al suo interno si svolge un insieme di processi, alcuni dei quali, come detto, vi nascono e vi terminano, altri coinvolgono, in entrata o in uscita, processi di altre unità funzionali, altri ancora da questi ne sono invece coinvolti; le unità funzionali, come detto, non necessariamente appartengono al medesimo ente ma possono appartenere anche ad altri enti, presentando quindi nell'insieme una pluralità di situazioni.

Si è detto, forse in modo troppo generale, che le nuove soluzioni tecnologiche richiedono un approccio «sistemico»: in realtà, più propriamente, sono alcune loro caratteristiche che lo richiedono, soprattutto se si vuole usufruire di tutte le opportunità e i vantaggi che le tecnologie, soprattutto quelle più recenti, mettono a disposizione. Tra queste caratteristiche vi sono, ad esempio, la possibilità di rendere disponibile, per un determinato problema, la medesima soluzione per tutti gli utenti interessati, in logica «uno a molti», accessibile da qualsiasi località si trovino gli utilizzatori: le soluzioni in modalità *cloud computing*, proprio, ad esempio, per la possibilità che offrono di evitare ridondanze e ripetizioni, richiedono appunto un approccio «sistemico» basato sull'analisi per processi che, per le sue caratteristiche, permette l'individuazione degli «elementi unici» in termini di utilizzatori e di dati. Conseguentemente l'utilizzo di soluzioni in *cloud computing* o, più in generale, l'occasione di un piano d'implementazione di soluzioni in *cloud computing*, possono rappresentare uno dei fattori abilitanti una visione sistemica ed uni-

taria dell'organizzazione in cui si opera e di quelle con cui questa si correla. Con riferimento alla pubblica amministrazione, ciò significa arrivare a definire linee architetturali e applicative che permettano un più efficiente svolgimento delle attività, sia di *back end* sia di *front end*.

2.2 Il metodo

Un processo è una sequenza di azioni e attività che devono essere svolte secondo un preciso piano procedurale e organizzativo: l'analisi per processi si sviluppa secondo un approccio logico che tende a fornire una visione esaustiva e integrata dei flussi informativi, delle fasi che li costituiscono e delle relazioni di tipo *input/output* che sono instaurate tra loro.

Le attività da svolgere sono pertanto:

– l'individuazione senza ambiguità del processo e la sua definizione univoca;

– l'analisi del processo.

Occorre quindi dapprima determinare con precisione il processo, ciò di cui ci si occupa, l'oggetto dell'analisi, eliminando gli elementi che potrebbero indurre a equivoci e quindi procedere ad una sua definizione che ne spieghi in modo esaustivo ma sintetico scopi e finalità.

Il secondo passaggio, cioè l'analisi, consiste nella descrizione del «contenuto» del processo, cioè nell'individuazione della sua «origine», della sua «destinazione» e dei punti di ingresso e uscita (percorso «fisico») ed il suo «sviluppo», intendendo con ciò chi lo svolge, chi ne è responsabile, chi viene interpellato e chi deve sapere che il processo è in corso (percorso «funzionale-amministrativo»): un simile approccio permette di determinare le relazioni esterne al processo in esame, ma anche la sua «struttura», cioè l'eventuale presenza di sotto-processi, cui ovviamente vanno applicati i medesimi criteri e metodi di analisi.

Preliminare è tuttavia la definizione di un modello logico e generale applicabile all'ambito che si vuole analizzare, che fornisca gli strumenti di «catalogazione» delle attività, i necessari vincoli di riferimento e le opportune chiavi interpretative, astraendo dalle specifiche e contingenti situazioni. Il modello logico, pur se a un elevato livello di astrazione, deve essere un vero e proprio strumento di analisi e di catalogazione delle rilevanze che via via l'analisi evidenzia e in quanto modello logico astratto, deve essere valido per ogni tipo di ente omogeneo e per ogni livello a cui si svolge l'analisi, avendo quindi carattere di generalità ed esaustività.

Appare evidente come la realizzazione di una simile attività di analisi su tutta la pubblica amministrazione centrale e locale presenti difficoltà praticamente insormontabili, soprattutto se la si vuole realizzare in una sola volta: l'unico approccio possibile è di tipo graduale, in termini sia di enti da analizzare sia di «livello» di approfondimento dell'analisi, partendo cioè da un sottoinsieme di enti e da una visione macro dei loro processi per, successivamente, da un lato approfondire l'analisi ai livelli inferiori e, dall'altro, espanderla ad altri enti. D'altro canto la presente trattazione non vuole avere carattere di esaustività ma, da un lato, esemplificare quali aspetti un'effettiva ed efficace attività di analisi possa mettere in luce, con lo scopo di individuare le criticità che con il processo di informatizzazione si dovranno affrontare, dall'altro suggerire un possibile metodo di analisi per superare i limiti e i difetti riscontrati nel processo di diffusione delle tecnologie Ict nella pubblica amministrazione.

La descrizione del metodo non è tuttavia completa: per definire una «architettura applicativa» basata su un'analisi per processi, non è infatti sufficiente fornire criteri rivolti a individuare i processi e le loro relazioni funzionali, ma occorre altresì individuare i criteri per definire una scala di priorità tra i processi stessi: da questo punto di vista gli enti della pubblica amministrazione presentano delle peculiarità che mettono in risalto la differenza di approccio necessaria rispetto ad organizzazioni di altri settori di mercato; in ambito aziendale la determinazione delle priorità è legata sia alla specifica attività svolta dall'organizzazione (in un'azienda che si occupa della catena del freddo è evidente che i processi avranno una sequenza di priorità differente da quella dei processi di un'azienda che produce automobili) sia alle scelte strategiche del *management*. Entrambi gli aspetti negli enti della pubblica amministrazione sono assenti: gli

enti dei differenti tipi svolgono attività diverse, ma le diversità non generano la possibilità di definire priorità tra i processi che non sono definibili neppure all'interno di un medesimo ente: in base a quale criterio è possibile definire più o meno prioritario un processo di gestione di un «permesso di costruzione» rispetto ad un processo di «gestione degli asili» all'interno di un comune o ad un processo di gestione di una cartella clinica in una azienda ospedaliera? Né, d'altra parte, i dirigenti degli enti pubblici hanno discrezionalità per definire priorità tra processi, per lo meno la legislazione attuale non lo consente. Il caso citato della cartella clinica può far sorgere dei malintesi: in relazione all'ambito sanitario, non si vuol infatti affermare che la gestione del pronto soccorso, in quanto maggiormente critica, non ha «priorità» maggiore rispetto alla gestione della farmacia, o per lo meno non è di questo significato di priorità che qui si discute; l'ottica è quella del sistema informativo e dei criteri che lo devono informare: da questo punto di vista non ci sono priorità tra i processi degli enti pubblici, in quanto questi si svolgono per «linee parallele», come appunto la gestione del pronto soccorso e quella della farmacia.

2.3 Il modello per l'analisi

Il primo aspetto da definire, o meglio da descrivere, è la missione dell'ente pubblico di cui ci si occupa. S'intende con ciò la descrizione sintetica delle finalità e degli obiettivi che gli sono propri, la loro caratterizzazione in termini tattici o strategici e la definizione del suo «bacino» di riferimento, in termini di destinatari dei risultati della sua attività. Si tratta quindi di una descrizione qualitativa e sintetica, che contiene le informazioni essenziali e necessarie a «comprendere» l'ente di cui ci si vuole occupare, comunque non descritte secondo una struttura formale rigidamente predefinita.

Il secondo aspetto è definire il modello teorico che permetta di analizzare, secondo un metodo preciso ed univoco, la «struttura» funzionale ed operativa dell'ente, cioè le modalità con cui svolge le proprie attività per il perseguimento della sua missione: l'analisi viene facilitata adottando un modo di procedere «alternato» dal «grande» (l'ente, una sua componente organizzativa) al «piccolo»

(la funzione, l'attività specifica) e dal «piccolo» al «grande», secondo un processo di astrazione che generalizza I risultati dell'analisi; è più semplice, da un punto di vista pratico, considerare, in partenza, delle «entità», delle attività così come oggi sono rappresentate ed organizzate, e individuarne le loro componenti, considerando che l'insieme delle attività svolte da un ente pubblico, come da una qualsiasi organizzazione, può comunque essere scomposto in attività «elementari», astraendo dalle realtà contingenti e specifiche dei singoli enti; queste attività «elementari», invertendo la «direzione» del processo ma sempre seguendo una percorso di astrazione, possono essere raggruppate in nuove «entità» che ricompongono in un ordinamento logico e sequenziale le varie attività elementari, cioè i processi.

Qualunque sistema, come può essere un ente della pubblica amministrazione, opera in un contesto determinato:

– da un insieme di *regole*, scritte o meno, rivolte a normare sia il funzionamento del sistema stesso sia le sue relazioni con il «mondo» in cui il sistema opera;

– da *atti* da perseguire, da compiere, sempre in relazione al mondo cui si rivolge;

– da *mezzi*, strumenti, materiali o immateriali che siano, da utilizzare per il perseguimento dei propri atti.

Per qualunque ente pubblico (amministrazioni centrali dello stato, regioni, province, comuni, comuni metropolitani, comunità montane e aziende sanitarie ed ospedaliere), sono quindi tre i cardini che concorrono allo svolgimento dell'attività dell'ente, con le naturali specificità a seconda del tipo di ente. Procedendo ad una descrizione dei tre cardini, si può dire:

– le *regole* sono l'insieme delle norme (leggi, delibere, o quant'altro) prodotte dai vari enti per determinare e disciplinare la loro attività ed il comportamento dei soggetti (individui, imprese, altri enti) compresi nella loro sfera di competenza o con cui sono in relazione; il sistema complessivo di regole che viene generato produce una struttura gerarchica (giuridicamente «gerarchia delle fonti»): i comuni, nell'emanazione di proprie regole, devono tenere conto di quelle emanate dalle regioni e dallo stato, le regioni di quelle ema-

nate dallo stato; il cardine delle regole non è suddiviso in aree differenti e la sua produzione ha carattere di trasversalità. Il cardine delle regole definisce anche le relazioni e i vincoli tra gli altri cardini e le aree di attività ove operano, a qualunque titolo, i soggetti, individuali o collettivi;

– gli *atti*, cioè gli obiettivi concreti da perseguire, derivanti dall'insieme delle attività svolte coerentemente con la missione dell'ente, sono solitamente rivolti all'esterno dell'ente stesso, e si concretizzano nell'erogazione di servizi materiali o immateriali a cittadini, imprese e, più in generale, a tutti i soggetti, individuali o collettivi, che rientrano tra i destinatari dell'azione dell'ente; i servizi sono finalizzati sia a permettere lo svolgimento delle attività dei destinatari sia a garantire che tali attività si svolgano in un contesto di correttezza reciproca secondo quanto stabilito dal sistema delle regole. Vi possono essere atti alla cui realizzazione concorrono più enti, anche di tipo diverso. L'insieme delle attività contenute nel cardine degli atti può essere raggruppato in due *ambiti di destinazione* dei servizi: ogni ente, indipendentemente dal tipo e con minore o maggiore efficacia e completezza, destina infatti i servizi al territorio e/o alla popolazione; gli atti da perseguire, quindi i servizi da erogare, sono ovviamente differenti a seconda dell'ambito cui sono rivolti e dell'ente che li eroga (ad esempio lo Stato non si occupa di certificati anagrafici e i comuni non si occupano di difesa); secondo il percorso di analisi indicato si ha che ogni ambito di destinazione si può articolare in una pluralità di *aree funzionali* che generalmente individuano insiemi e/o categorie di servizi, relativamente omogenei al loro interno, che tendenzialmente sono in corrispondenza con le strutture organizzative degli enti (unità funzionali). Le singole aree funzionali si articolano in *aree-servizio*, che rispondono comunque ad obiettivi generali e strategici comuni: a questo livello vengono erogati i servizi; lo schema proposto diviene particolarmente fecondo seguendo i vari livelli di analisi, in quanto è in questo «percorso» che si possono individuare le relazioni, funzionali ed operative, che le unità funzionali dell'ente intrattengono tra loro e/o con unità funzionali di altre amministrazioni piuttosto che, più in generale, con il mondo esterno all'ente stesso, per l'espletamento delle proprie funzioni ed attività finalizzate alla missione dell'ente;

– i *mezzi* sono l'insieme delle risorse umane ed economico-finanziarie che gli enti reperiscono e utilizzano per il loro funzionamento e per l'espletamento dei loro atti. Il cardine dei mezzi si articola, come emerge dalla stessa definizione, nelle due medesime macroaree che lo definiscono, indipendentemente dal tipo di ente: i processi per il reperimento dei mezzi finanziari possono essere diretti (imposte e tasse) o indiretti (trasferimenti finanziari da altri enti sovra ordinati): lo stato utilizza solo processi diretti, gli altri enti utilizzano entrambi; per le risorse umane i processi di reperimento sono analoghi tra gli enti e riconducibili ai concorsi. Le due aree richiedono attività di pianificazione dei bisogni e rivestono un ruolo di attività secondarie rispetto alle precedenti, permettendone la realizzazione. L'ambito cui i mezzi sono rivolti è naturalmente lo stesso ente.

Il terzo aspetto, infine, riguarda le finalità delle attività svolte dagli enti, che possono essere:

– *strategiche*, relative ai processi destinati al raggiungimento della missione dell'ente, al supporto alla regolamentazione dell'operare dell'ente stesso e del sistema nel suo complesso; ogni tipo di ente ha proprie finalità strategiche come anche ogni singolo ente, finalità che vengono perseguite all'interno degli ambiti e delle competenze specifiche;

– *operative*, relative ai processi destinati direttamente all'erogazione concreta di servizi, sia materiali e tangibili sia immateriali, a cittadini ed imprese;

Ogni ente svolge le proprie attività all'interno dei confini territoriali che gli sono propri e che sono definiti dal sistema delle regole.

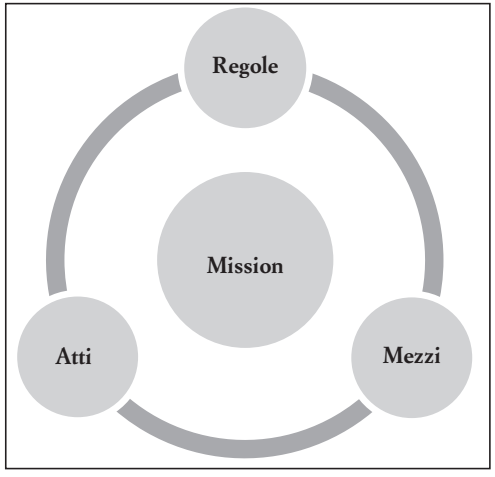
Lo schema generale di massima che deriva da quanto sopra definito può essere considerato il seguente:

Tabella 1. Schema generale

ENTE		
REGOLE	**ATTI**	**MEZZI**
	CITTADINI TERRITORIO	UMANI ECONOMICO-FINANZIARI

Un'altra rappresentazione dello schema che rappresenta, più sinteticamente, la mappa delle relazioni al massimo livello di sintesi è la seguente:

Figura 3. Mappa relazioni



Il risultato complessivo del processo di analisi descritto, cioè una sorta di «scomposizione» dell'ente nelle sue attività «elementari», costituisce la premessa per una successiva fase di «ricomposizione» delle attività secondo una vista integrata, che deve permettere l'eliminazione delle attuali false «barriere» che esistono tra le diverse unità funzionali e che tendono a darne l'immagine di «silos» procedurali distinti; la «ricomposizione» deve mettere al centro della visione il destinatario dei servizi e le sue necessità di rapporto con le amministrazioni, non l'erogatore dei servizi, come sostanzialmente è oggi: ciò permette di ricostruire, riorganizzandoli sul piano logico e funzionale, i processi, disponendoli in una sequenza di azioni e attività articolate secondo un preciso piano procedurale e organizzativo integrato, rivolto a soddisfare integralmente le necessità del destinatario, con significative conseguenze sul piano dell'efficienza complessiva del sistema. Si consideri, a questo proposito, ad esempio il tema della ripetitività delle richieste di dati da parte delle amministrazioni pubbliche e, conseguentemente, delle attività che devono essere svolte dal cittadino; si possono fare due considerazioni sul risultato di questo modo di procedere: da un lato l'inevitabile proliferare di dati errati, dall'altro le conseguenze del trasferimento fisico dei dati: si può arrivare a doversi procurare più copie degli stessi dati e doverli consegnare in luoghi diversi, magari ad organizzazioni funzionali appartenenti tutti al medesimo ente: tutto ciò perché non vengono utilizzate concezioni delle organizzazioni e delle relative attività basate su processi, che evidenzierebbero immediatamente queste situazioni «patologiche». In ciò, evidentemente, si riflette una concezione dell'attività delle singole unità funzionali basata, come già accennato, su una «architettura» a «silos», in cui le attività non si «parlano», non hanno rapporti «trasversali» e sono concepite come auto-consistenti. L'attività di analisi descritta porta alla costruzione di un modello che rappresenta, in modo univoco, l'ente che si vuole analizzare, la sua struttura logico funzionale e il sistema di relazioni all'interno del quale svolge la propria attività: soprattutto quest'ultimo aspetto permette di ricostruire l'attività dell'ente secondo una struttura per processi, con significativo aumento dell'efficienza complessiva del «sistema ente».

Nel seguito vengono presentate alcune applicazioni di quanto esposto in precedenza, soprattutto con riferimento alle attività di «scomposizione»: scopo principale di questa parte dello studio è presentare sia un metodo, che possa aiutare ad analizzare in modo più efficace le attività degli enti pubblici, sia degli esempi di applicazione del metodo stesso; per questi motivi non ci si occuperà ne di tutti gli enti pubblici ne, per quanto riguarda gli enti trattati, di tutti i dettagli analitici delle loro attività e del loro sistema di relazioni: si sono scelti alcuni enti in quanto di particolare rilevanza rispetto al tema generale che viene trattato nel presente lavoro, e di questi enti si sono effettuate le analisi solo di alcune «aree specifi-

che».

Inoltre, per quanto riguarda l'attività di «ricomposizione», questa viene esemplificata ad un livello macro, riguardante l'intero ente: si cercherà cioè di rappresentare, ad esempio, il sistema delle relazioni esterne all'intero ente, senza scendere nel dettaglio di quale specifica unità funzionale si relazioni con quale unità funzionale di quale altro ente per lo scambio di quali dati, e si traccerà uno schema di massima per il sistema delle relazioni interne. Con ciò non si vuole in qualche modo «abdicare» alla teoria esposta in precedenza, tutt'altro, in quanto proprio l'applicazione di quella teoria ha permesso di tracciare il sistema delle relazioni di interesse, se pur ad un livello relativamente «alto».

3. La sanità

3.1. Il contesto generale

La struttura del comparto sanitario è decisamente complessa: comprende enti ai differenti livelli della struttura amministrativa, organizzazioni pubbliche e private, i cittadini e i professionisti del settore; i principali attori del sistema sanitario sono lo stato, le regioni, gli enti sanitari pubblici, le strutture sanitarie private accreditate presso il Sistema sanitario nazionale (Ssn), il sistema previdenziale, medici convenzionati con il Ssn ed i cittadini: tra questi intercorre un sistema di relazioni che può presentare delle differenze, anche significative, dovute alle diverse scelte legislative operate dalle regioni; in questa sede che, ha lo scopo di delineare dei modelli generali, in grado comunque di fornire elementi di valutazione e di riflessione sui temi di pertinenza dello studio, non si terrà conto di tali differenziazioni, anche in considerazione del fatto che tali elementi non incidono sull'applicazione del metodo proposto e sui risultati dell'analisi.

All'interno del sistema sanitario possono essere riconosciuti ruoli diversi e specifici per ogni attore, quali ad esempio tra gli altri, e in prima approssimazione:

– lo Stato (Ministero della salute) ha lo scopo di fornire la linee strategiche generali in materia sanitaria per l'intero paese e (Ministero dell'economia) di fornire le risorse economiche, alle regioni, per il funzionamento del sistema;

– le regioni hanno lo scopo di articolare sul proprio territorio le direttive nazionali, coniugandole secondo i propri orientamenti politici strategici in materia di sanità, di fornire gli enti sanitari locali delle necessarie risorse finanziarie e di vigilare sulle modalità di fornitura dei servizi sanitari;

– le strutture sanitarie locali, pubbliche o private, hanno lo scopo di erogare i servizi sanitari e di assistenza ai cittadini;

– i medici convenzionati con il Ssn hanno la funzione di fornire al cittadino l'assistenza primaria e di indirizzarlo, nel caso, alle opportune strutture specialistiche;

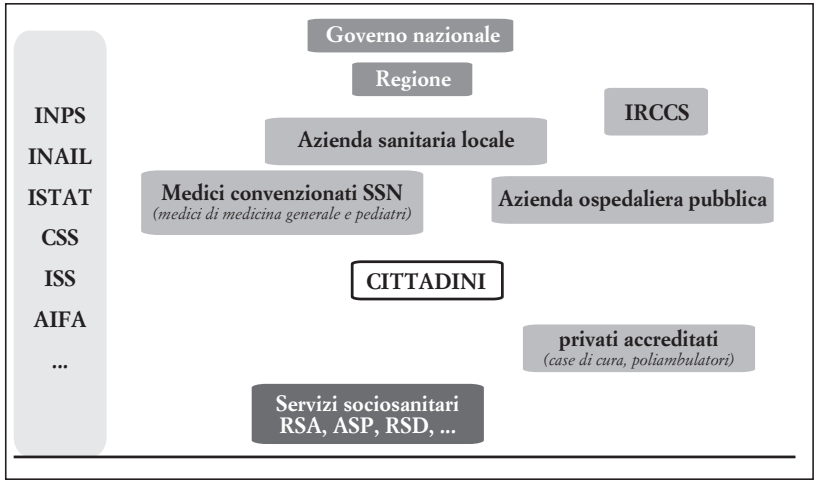
– i cittadini sono da un lato i «finanziatori» del sistema sanitario, tramite il versamento delle imposte, e dall'altro i fruitori dei servizi forniti, in qualità di «pazienti».

I soggetti citati possono essere considerati il nucleo del sistema, che tuttavia comprende o entra in contatto con numerosi altri organismi o enti: si pensi ad esempio a strutture come l'Istituto superiore di sanità o, come già detto, gli enti del sistema previdenziale che provvedono alle prestazioni monetarie in caso di malattia o maternità; si considerino inoltre i molti punti di contatto (o di auspicabile maggior integrazione) con il sistema dell'assistenza sociale.

Lo schema che segue rappresenta una mappa del sistema, certamente incompleta e approssimativa, ma utile come schema di riferimento per una prima analisi. Anche in questa versione molto semplificata appare evidente sia l'elevato numero dei soggetti coinvolti sia la loro grande differenziazione[1].

[1] Gli enti citati nella mappa alla pagina seguente sono: Inps; Inail, Istat, Css (Consiglio superiore di sanità), Aifa (Agenzia italiana per il farmaco), Irccs (Istituti ricovero e cura a carattere scientifico), Rsa (Residenza sanitaria assistenziale), Asp (Azienda di servizi alla persona), Rds (Residenza sanitario assistenziale per disabili).

Figura 4. Mappa generale del sistema sanitario



Tre aspetti devono essere ancora presentati per inquadrare meglio il settore e delinearne alcune caratteristiche specifiche di cui, in una prospettiva di informatizzazione di un «sistema sanitario nazionale» occorrerebbe tenere conto, per le conseguenze e gli effetti sul piano delle relazioni tra enti, soprattutto con riferimento all'azione di «monitoraggio» delle attività sanitarie e di gestione del sistema dei finanziamenti:

– considerato come «mercato», intendendo con ciò il luogo d'incontro tra il paziente e la struttura di cura, il settore sanitario presenta una caratteristica particolare, cioè quella dell'asimmetria informativa: con ciò si vuol dire che il paziente non ha gli strumenti conoscitivi per capire la malattia da cui è affetto ed individuare le susseguenti cure: deve ricorrere ad un intermediario (il medico) che lo indirizza alla cura di cui necessita. In questo è appunto asimmetrico in quanto necessita della presenze di «intermediari» che favoriscono l'incontro tra gli attori del «mercato» (relazione cittadino-medico-struttura sanitaria);

– la stessa definizione della fornitura, o del prodotto, è complessa in quanto dipende da diversi parametri: una determinata prestazione sanitaria risulta più o meno complessa a seconda che sia erogata a un giovane, un anziano o ad una persona che soffra anche di un'altra malattia; in realtà si è di fronte a tre differenti «prodotti» che hanno costi differenti e quindi prezzi (rimborsi) a loro volta differenti: a questo va aggiunto un ulteriore parametro dato dalla struttura e dalla persona, o meglio, in questo caso, dal suo livello di specializzazione ed esperienza, che eroga il servizio (relazione cittadino-malattia-costo);

– il sistema dei finanziamenti è basato su due fasi successive: il finanziamento delle regioni «per quota *pro capite*», basato sulla struttura della popolazione rispetto all'età (il principio è che anziani e molto piccoli sono più facilmente soggetti ad ammalarsi, e quindi più «costosi») ed il finanziamento alle strutture sanitarie locali, basato sul sistema dei Drg, cioè su un insieme di costi normalizzati, definiti per le varie prestazione sanitarie prestate (relazione cittadini-morbilità-costi).

Ai fini dello sviluppo dell'analisi, nel seguito ci si occuperà degli ospedali e della loro struttura organizzativa di massima, per successivamente sviluppare un progetto di fascicolo sanitario elettronico, data la rilevanza che riveste ai fini della cura dei cittadini, come emergerà nel seguito.

3.2. L'ospedale

L'attuale struttura organizzativa di un ospedale, pubblico o privato, è basata su una concezione anatomo-funzionale dell'azione di cura, nel senso che l'aspetto anatomo-funzionale della patologia determina il luogo fisico della cura: l'ospedale è cioè organizzato per curare l'organo malato, indipendentemente dalla gravità della malattia; d'altra parte se si pensa all'organizzazione di un ospedale si osserva che questa è basata su «specialità» di carattere anatomo-funzionale che si traduce nei corrispondenti reparti, quali quelli di oculistica, cardiologia, pneumologia piuttosto che di ostetricia, di urologia o di otorinolaringoiatria, al cui fianco vi sono altri reparti con funzione di servizio, quali il laboratorio di analisi, la radiologia, il blocco operatorio, la rianimazione o la farmacia. Tra queste strutture vi è, escludendo le componenti di natura amministrativa, un complesso sistema di flussi informativi a carattere clinico che hanno

al loro «centro» il malato, il paziente e che trovano la loro «concretizzazione» ed il loro supporto nella cartella clinica e la loro sintesi nel fascicolo sanitario, tema su cui si tornerà successivamente.

Prima di rappresentare, sinteticamente, gli schemi generali di un ospedale è utile richiamare brevemente alcuni nuovi recenti orientamenti in tema di organizzazione sanitaria ed ospedaliera in quanto, nella prospettiva del presente lavoro, questi nuovi orientamenti, nel momento in cui saranno tradotti in atti concreti, potranno dare origine a profonde modifiche nelle logiche dei sistemi informativi ospedalieri; si è detto dell'orientamento anatomo-funzionale dell'organizzazione ospedaliera attuale, che porta ad una organizzazione di cura per «organo» soggetto a patologia: alcune recenti orientamenti medici e scientifici tendono, al contrario, a individuare un'organizzazione delle strutture ospedaliere per «gravità» del fatto patologico e quindi per livello di intensità di cura, con la conseguenza che le specialità, al di là dell'essere eliminate, non possiedono più un loro «territorio» di azione (il reparto) ma svolgono attività di servizio verso i differenti reparti, organizzati per livello di gravità della patologia. D'altra parte un esempio di come il criterio anatomo-funzionale sia in qualche modo superato già nelle organizzazioni sanitarie attuali, è dato, ad esempio, dal reparto «malattie infettive»: nel reparto vengono ricoverati malati di patologie diverse in base al criterio dell'infettività della patologia, che è il vero problema sanitario da fronteggiare, con il supporto delle specialità che intervengono per quanto è di loro competenza; analoghe considerazioni possono essere svolte a proposito del reparto di rianimazione, che vede ricoverati malati legati a determinati stati di rischio di vita, non a determinate patologie. Questi nuovi orientamenti vedono anche l'ospedale come struttura «tecnologicamente avanzata, dotata di strumentazione di eccellenza e luogo ove il malato deve permanere il tempo strettamente necessario alla cura della sua fase acuta. La funzione territoriale dell'ospedale, attuata dai suoi bracci operativi sul territorio, riguarderà l'attività di diagnosi e cura di primo e secondo grado di complessità e l'erogazione di servizi post-acuzie intermedi fra l'ospedale e il domicilio. Per tale riqualificazione, dovranno essere implementati modelli organizzative gestionali in rete per funzioni, atti a realizzare forme di continuità assistenziale comprendendo anche l'ospedalizzazione domiciliare e forme alternative al ricovero, presidiando il raccordo con le cure domiciliari socio sanitarie. Per la gestione territoriale sanitaria e socio sanitaria e per la gestione delle patologie della cronicità sarà,quindi, garantita la continuità del processo di diagnosi e cura programmato nella filiera domicilio-territorio-ospedale-territorio-domicilio. La complessiva riqualificazione della rete di offerta dei servizi sanitari e uno degli elementi strategici per adeguare il sistema sanitario alle esigenze del cittadino»[2].

La citazione, pur se lunga, è di estrema importanza ai fini dello studio, in quanto indica chiaramente quali dovranno essere le linee strategiche di sviluppo dei sistemi informativi sanitari, non tanto ospedalieri ma proprio sanitari, nel senso del superamento dell'attuale logica verso una logica che veda il malato oggetto e soggetto delle realizzazioni tecnologiche, anziché l'ospedale posto oggi in tale ruolo: va osservato che le soluzioni tecnologiche attuali in uso non sono in grado di supportare una tale modifica di prospettiva, proprio per la loro logica che vede al centro la gestione della struttura ospedaliera non del malato.

3.2.1 Gli schemi generali di un ospedale

Si riportano gli schemi generali di un ospedale, sviluppati secondo i criteri metodologici esposti nei paragrafi precedenti, schemi comunque basati sullo stato dell'arte attuale, non sulle evoluzioni organizzative e funzionali indicate in precedenza, in quanto non ancora definiti con esattezza, ma solo, per ora, ancora a livello di enunciazione strategica.

[2] Regione Lombardia, *Piano socio sanitario regionale 2010-2014*.

Figura 5. Ospedali – Ambito di destinazione: cittadini

Missione

Gli ospedali hanno l'obiettivo strategico di svolgere tutte le necessarie attività di diagnosi e cura del cittadino affetto da patologia in fase acuta (non si occupa quindi di stati patologici e di situazioni che necessitano di supporto riabilitativo o di assistenza a lungo termine, che vengono seguite in strutture di lungo degenza o in strutture a carattere socio-sanitario); la struttura ospedaliera ed il personale che vi opera devono preoccuparsi di effettuare una corretta diagnosi dello stato morboso per poter definire la corretta terapia e quindi soddisfare la missione.

Cardini

Regole

Gli enti sanitari locali non hanno potestà legislativa, bensì applicano le leggi statali e regionali di pertinenza; sono soggetti all'azione di programmazione e di vigilanza della regioni; per il loro funzionamento interno e per la gestione delle attività sanitarie sul territorio di competenza producono regolamenti organizzativi.

Atti

Ambito di destinazione: cittadini

Aree funzionali

Accettazione/Pronto Soccorso	**Aree-servizio:** non specifiche	
Blocco Operatorio	**Aree-servizio:** Chirurgia Generale Ostetricia Otorinolaringoiatra Oculistica	Chirurgia Plastica Cardiochirurgia Traumatologia
Anestesia/Rianimazione	**Aree-servizio:** non specifiche	
Radiologia/Medicina Nucleare	**Aree-servizio:** Radiologia Tomografia assiale computerizzata	Scintigrafia Risonanza Magnetica
Laboratori Analisi	**Aree-servizio:** Anatomia Patologica Microbiologia	Ematochimica
Farmacia	**Aree-servizio:** non specifiche	
Degenze e cura	**Aree-servizio:** Medicina Generale Geriatria Chirurgia generale Ostetricia-ginecologia Otorinolaringoiatria Oculistica Chirurgia plastica Pediatria	Neurologia Cardiologia Ortopedia/ Traumatologia Psichiatria Urologia Pneumologia

Missione

Cardini

Mezzi

Aree Funzionali

Area Economico-Finanziaria	**Aree-servizio:** Contabilità-controllo gestione Economato/ Approvvigionamenti
Area Personale	**Aree-servizio:** Personale Ufficio Infermieristico Formazione
Area Direzione Sanitaria	**Aree-servizio:** Assistenza Sociale Organizzazione Infermieristica Organizzazione Medica

Si è detto del ruolo della cartella clinica dal punto di vista dei flussi informative relative al paziente: vale la pena ritornare su quest'aspetto e su quelli a lui correlati per esplicitare i motivi che hanno portato a considerare il fascicolo sanitario come caso di particolare interesse per l'esemplificazione di realizzazione di soluzioni in *cloud*.

All'atto del ricovero di un cittadino viene compilata la cartella clinica con l'indicazione delle caratteristiche del suo stato morboso (anamnesi), delle cure prestate e delle decisioni prese dal medico, se ricovero o dimissione; nel primo caso, a seguito del ricovero nel reparto di competenza, il paziente viene sottoposto ai trattamenti sanitari del caso, che vengono registrati nella cartella clinica; al termine delle cure viene compilata la lettera di dimissioni, con le relative motivazioni, che va a costituire parte integrante della cartella clinica e che viene archiviata nell'ospedale; nel secondo caso viene compilata la lettera di dimissioni che segue l'iter precedente. Ad ogni fatto morboso che colpisca un cittadino viene seguito il medesimo iter, con la compilazione di una nuova cartella clinica. È tuttavia da osservare che i dati sanitari di un cittadino non originano esclusivamente dalle cartelle cliniche, che anzi intervengono nel solo caso di

ricovero ospedaliero, ma da diverse altre situazioni, che vanno dalle visite del medico di base agli esami o controlli effettuati presso laboratori o centri specialistici. Il fascicolo sanitario è, concettualmente, lo strumento di raccordo di tutte li informazioni sanitarie di un cittadino, indipendentemente da dove siano state generate e dove siano conservate.

Nella prospettiva dello studio, che vede centrali i flussi informativi che caratterizzano gli enti, si rivela quindi determinante il caso del fascicolo sanitario in quanto strumento di comunicazione per eccellenza di tutto il mondo sanitario. Nel seguito si tratterà del progetto di fascicolo sanitario elettronico e di possibili modalità di implementazione secondo logiche di *cloud computing*. La descrizione del modello di Fse che è stato messo a punto e che è riportata nel seguito, mostra come lo strumento così concepito vede al centro il cittadino nella sua accezione di «paziente», rispondendo così alle esigenze di centralità del malato secondo i nuovi orientamenti medici e scientifici riportati in precedenza; la soluzione tecnologica indicata risponde ad un fondamentale requisito implicito in tali nuovi orientamenti, cioè l'accessibilità ai dati sanitari del paziente da parte di tutto il personale autorizzato che ha in cura il cittadino, da qualunque luogo fisico e con qualunque apparecchiatura tecnologica.

3.3 Il fascicolo sanitario elettronico

La scelta del Fse è motivata, come indicato sopra, dal ruolo chiave che svolge nei flussi che riguardano il cittadino nella sua qualità di «paziente» e, quindi, sia dall'importanza che la sua implementazione è destinata ad avere nell'organizzazione e nello svolgimento delle attività sanitarie sia, di conseguenza, dalle aspettative che il Fse stesso suscita negli operatori sanitari e nei cittadini, che vedrebbero semplificate e rese più efficienti le loro relazioni con il sistema sanitario. Il tema dell'implementazione del Fse è all'attenzione dei responsabili sanitari delle regioni, delle aziende sanitarie sia locali sia ospedaliere e del Ministero della salute ormai da molti anni; le aspettative legate alla sua realizzazione sono, come già detto, molto alte in quanto si realizzerebbe un vero e proprio salto qualitativo

nelle modalità di erogazione e fruizione dei servizi sanitari ed assistenziali; i vantaggi previsti sono infatti numerosi: riduzione nella duplicazione delle analisi e degli accertamenti sanitari, con conseguente riduzione della spesa sanitaria, possibilità per i medici di consultare tutte le informazioni cliniche relative ad un determinato paziente e quindi di effettuare facilmente anche consulti con altri colleghi, possibilità per il cittadino di consultare la propria situazione e storia sanitaria ovunque si trovi, non necessariamente dal comune o dalla regione di residenza, riduzione per i cittadini del tempo perso per le file agli sportelli, con riduzione delle liste di attesa; questi sono solo alcuni dei benefici attesi che, certamente, farebbero modificare significativamente in meglio i rapporti tra cittadini e sistema sanitario, oggi non sempre efficienti e positivi.

Il fascicolo sanitario trova «alimentazione», in termini di informazioni che permette successivamente di reperire, nelle applicazioni dell'area «clinica» e precisamente:

– centro unico di prenotazione (Cup)
– pronto soccorso
– accettazione, dimissioni, trasferimento, (Adt)
– blocco operatorio
– cartella clinica infermieristica
– cartella clinica medica
– dossier sanitario
– laboratori di analisi (Lis)
– radiologia (Ris)
– anatomia patologica
– trasfusionale,

che forniscono le informazioni, provenienti dalle Asr[3], necessarie alla costituzione del fascicolo stesso.

A queste occorre aggiungere
– le prescrizioni elettroniche per visite specialistiche
– le prescrizioni elettroniche per i farmaci

[3] Con l'acronimo Asr sono considerate sia le aziende sanitarie locali e sia quelle ospedaliere.

– il *patient summary*[4]

che vengono prodotti dai medici di medicina generale (Mmg) e dai pediatri di libera scelta (Pls), poiché queste informazioni vanno a completare il fascicolo sanitario elettronico del paziente.

3.3.1. Il procedimento utilizzato

Stante l'obiettivo di delineare una soluzione applicativa e determinare i relative valori di costo, si è proceduto a raccogliere informazioni e dati reali, con riferimento alla applicazioni dell'area clinica, presso regioni che hanno allo studio o stanno implementando progetti di Fse, presso alcune Asr e presso alcuni Mmg e Pls; quest'attività di confronto con alcuni enti regionali ed aziende ha inoltre permesso di individuare nell'azienda sanitaria locale od ospedaliera, nel cittadino e nel medico le unità di calcolo per la determinazione dei costi. In particolare per quanto riguarda i costi per il collegamento di Mmg/Pls al Fse sono state considerate le esperienze di alcune regioni che hanno avviato, nel corso degli ultimi dieci anni, significativi progetti di rete che hanno coinvolto i medici di base. I dati di spesa raccolti sono stati normalizzati e generalizzati a tutte le realtà regionali e a tutte le Asr, con ciò evidentemente è stata effettuata una parziale semplificazione che, tuttavia, non inficia significativamente i risultati finali, che quindi possono essere assunti come un'approssimazione accettabile e ragionevole del valore ricercato.

Per la valutazione dei costi, sia d'implementazione sia di gestione e manutenzione, si è sviluppato un «modello» che prevede di dotare tutti i cittadini del Fse; del «modello» si sono effettuate le stime di costo di implementazione e di gestione, secondo due scenari:

– un primo scenario di tipo «conservativo», in cui si suppone di mantenere l'esistente, in termini di soluzioni Ict presenti presso regioni e Asr, di effettuare per tutte le Asr le attività di sviluppo della componente «fascicolo sanitario» e, conseguentemente, quelle di adeguamento ed integrazione della soluzione fascicolo con le soluzioni Ict esistenti nelle Asr;

– un secondo scenario di tipo «evolutivo», in cui si suppone di

[4] Il *patient summary* è la sintesi della storia del paziente descritta dagli Mmg/Pls.

dotare *ex novo* le Asr di un nuovo *software* standard per l'area fascicolo sanitario, al fine di consentire l'adozione di soluzioni basate su *cloud*, difficilmente adottabili nel caso precedente, data l'estrema variabilità dei software installati nell'area clinica delle Asr, variabilità che comunque sarebbe destinata a rimanere.

A questo proposito va osservato che, come tutte le attività di modellazione, anche questa presenta limiti dovuti alla necessaria schematizzazione e semplificazione che ogni modello comporta, e che vengono espresse dalle ipotesi che stanno alla base del modello stesso: d'altro canto la costruzione di un modello è un'attività di simulazione della realtà che, come in questo caso, può essere molto complessa; è proprio l'intrinseca complessità che porta ad utilizzare un modello per determinate valutazioni, in quanto queste potrebbero essere estremamente difficoltose, se non addirittura impossibili, se effettuate «direttamente» sulla realtà: un modello non deve quindi essere una copia «esatta» della realtà, ma una sua «approssimazione», che risulti coerente e ragionevole con le ipotesi che si sono assunte e che permetta di effettuare valutazioni in un contesto logicamente coerente.

È evidente che un progetto delle dimensioni e della complessità di quello descritto nel seguito, deve essere disegnato come un percorso d'implementazione progressiva delle sue componenti e deve anche prevedere la realizzazione di iniziative propedeutiche, in funzione del diverso grado di automatizzazione dei singoli enti sanitari. In questa sede tuttavia non ci si propone di definire un vero e proprio piano per l'implementazione del progetto, ma ci si pone un obiettivo differente e, precisamente, di darne una descrizione indicativa per arrivare a una «misura» economica del progetto stesso indipendentemente, appunto, dalla tempistica e dalle fasi della sua realizzazione e dalle reali situazioni dei singoli enti coinvolti, al fine di valutare l'effetto che il *cloud computing* potrebbe avere in termini di riduzione della spesa: a tal fine sono ovviamente accettabili alcune schematizzazioni e semplificazioni purché dichiarate, come appunto in questo caso.

I due scenari, ed il modello su cui sono basati, sono preceduti da una breve analisi dello stato attuale, prevalentemente di carattere

qualitativo dato che la situazione corrente è caratterizzata da forti disomogeneità, da realizzazioni parziali e non completamente coerenti tra loro dal punto di vista degli obiettivi generali, che dovrebbero necessariamente essere comuni; sulla base della informazioni raccolte, si è inoltre proceduto ad effettuare una stima complessiva delle spese sostenute sino ad oggi relativamente al solo Fse, senza quindi considerare altre componenti, quali carta sanitaria o altre iniziative, non strettamente attinenti alla realizzazione del Fse.

3.3.2. Lo scenario attuale

L'analisi dello scenario attuale, basata su una ricognizione rivolta a caratterizzare nei suoi tratti principali lo stato dell'arte, mostra come, ad oggi, la situazione non si presenti particolarmente positiva od omogenea: non tutte le regioni hanno iniziato ad investire nell'implementazione del progetto di Fse, tra le regioni in cui i lavori sono iniziati vi è una situazione di notevole disomogeneità nel grado di sviluppo, i progetti non sempre sono completamente compatibili dal punto di vista applicativo, e risulta anche che vengano utilizzati standard differenti; questi ultimi aspetti rendono problematico uno dei punti caratterizzanti e qualificanti del Fse e cioè l'accessibilità ai dati sanitari da qualunque punto del paese: in altre parole non pare che le singole realizzazioni si stiano sviluppando all'interno di un progetto globale e di un conseguente coordinamento a livello nazionale. Solo nel 2011 il Ministero della salute ha definito delle *Linee guida sul fascicolo sanitario elettronico*, ma nel frattempo diverse regioni avevano già avvito delle realizzazioni del Fse secondo linee proprie.

A qualificare meglio la situazione è utile analizzare i dati resi disponibili dalla Federazione italiana delle Asr e dal Ministero della salute che, se pur non recentissimi (risultano pubblicati nel 2010), sono comunque gli unici disponibili; da questi dati emerge che:

– 3 regioni dichiaravano di avere il Fse a disposizione delle Asr e degli operatori sanitari per oltre il 75% dei casi;

– 4 regioni dichiaravano di avere il Fse a disposizione delle sole Asr per il 75% dei casi;

– 7 regioni dichiaravano di avere il Fse a disposizione delle Asr e degli operatori sanitari per meno del 25% dei casi;

– per le restanti regioni non si avevano dati o la situazione era intermedia rispetto ai casi indicati in precedenza;

– il 43% delle aziende locali e il 62% delle aziende ospedaliere dichiaravano di interagire «in qualche modo» con il fascicolo elettronico;

– il 71% dei medici di famiglia e dei pediatri di libera scelta, il 67% dei medici ospedalieri e specialistici, il 19% degli infermieri e solo il 5% dei farmacisti erano in qualche modo al corrente o utilizzavano il fascicolo elettronico;

– per quanto riguarda le prestazioni sanitarie il 52% di quelle specialistiche ed ospedaliere, il 33% di quelle farmaceutiche ed il 24% di quelle di pronto soccorso sarebbero state gestite tramite Fse;

– complessivamente solo il 43% delle regioni dichiarava di gestire almeno una parte dei propri servizi con l'ausilio del Fse, ma non in tutte la aree che lo compongono;

– in generale le regioni dichiaravano, tuttavia, che il progetto era ancora in fase sperimentale, accessibile solo al personale sanitario e non ancora ai cittadini.

I dati riportati evidenziano, dal punto di vista quantitativo e qualitativo, una situazione disomogenea che pare si stia sviluppando al di fuori di qualunque piano organico; in ogni caso non risulta all'attenzione di alcuna regione il pur evidente fatto che frequentemente il cittadino viene curato presso strutture sanitarie al di fuori della regione di residenza, o in strutture private, e le implicazioni che questo fatto può avere per la costruzione di un unico fascicolo per lo stesso paziente, indipendentemente dalla provenienza dei dati sanitari; da un punto di vista qualitativo è inoltre molto interessante analizzare come le singole regioni presentino il proprio progetto di Fse:

– Regione Lombardia: la presentazione del Fse ha una decisa ottica «regionale», viene indicato il *network* sanitario regionale come fonte dei dati, l'utilizzo prevalente è rivolto al personale sanitario che ha in cura un determinato paziente e si lasciano tuttavia a prossimi sviluppi l'accessibilità ai dati del Fse anche da parte dei cittadini (con possibilità di modifica controllata dei dati) e si dichiara la disponibilità all'apertura sia a reti nazionali che internazionali (europee);

– Regione Toscana: enfatizza molto il ruolo del cittadino, sia come utilizzatore in qualunque momento dei propri dati clinici, che come autorizzatore alla creazione o meno del Fse, all'immissione dei dati o alla loro revoca; l'accesso ai dati è riservato ai medici, opportunamente autorizzati anche dal paziente, che operano in uno stato di emergenza del paziente;

– Regione Sardegna: il Fse risulta in fase sperimentale in due località, nasce alla luce dei risultati del gruppo di lavoro interregionale coordinato dal Dipartimento per l'innovazione e le tecnologie e viene collocato all'interno di una strategia architetturale di riferimento per il sistema nazionale della sanità elettronica;

– Regione Liguria: il Fse, chiamato «Conto corrente salute», pare presentare una visione più ampia rispetto ad altri casi, in quanto rivolto anche ad alcune attività di tipo istituzionale (campagne informative ed epidemiologiche, ecc.) ed amministrative;

– Regione Emilia-Romagna: l'utilizzo del Fse è rivolto al personale sanitario, ma anche in questo caso il cittadino ha piena autonomia su di esso (può anche oscurare documenti che ritiene – con quale competenza medica? – non debbano essere visti dal personale sanitario «regionale»).

Quest'ultimo punto pone un problema particolare che vale la pena discutere brevemente: il Garante per la privacy ha emanato, nel luglio 2009, le linee guida in relazione al Fse stabilendo la necessità del consenso, da parte del cittadino, alla creazione e alimentazione del Fse stesso e la possibilità, sempre per il cittadino, di oscurare/rendere visibile la propria documentazione clinica nei confronti dei professionisti sanitari. Il Ministero della salute, nel novembre 2010, si è adeguato a tale direttiva, integrandola con la necessità, per il cittadino, di dare specifici consensi «sia sulle informazioni da rendere visibili o meno, sia sui soggetti del Ssn che hanno in cura l'assistito da abilitare all'accesso ai dati contenuti nel Fse»; ha inoltre aggiunto la possibilità, sempre per il cittadino, di inserire, a propria discrezione, dati ed informazioni personali, file di documenti sanitari, un diario degli eventi sanitari rilevanti o promemoria per i controlli medici periodici; il Ministero precisa tuttavia che queste informazioni «arricchiscono il Fse» ma che «risultano non certificate». I problemi legali che nascono da queste indicazioni sono innumerevoli, ma comunque la loro trattazione esula dal contesto del presente studio: si sono brevemente illustrati anche questi aspetti unicamente per accennare a tutta una serie di altri problemi che devono essere risolti prima di far intervenire la tecnologia (ad esempio non risulta che si sia posto il problema di come poter gestire i vari consensi in modo omogeneo a livello nazionale, evitando che il cittadino sia costretto ad esprimere, cambiando regione[5], molteplici consensi per la creazione del Fse e l'utilizzo dei dati ivi contenuti). Il tema del consenso e della «certificazione» dei dati immessi nel Fse sono quindi di particolare rilevanza e complessità, anche sul piano legislativo; a questo proposito vale al pena ricordare l'esperienza di alcuni paesi europei a proposito del Fse ove questo viene considerato, sul piano legislativo, elemento necessario alla cura del cittadino: in tale modo il suo contenuto diviene «sanitario» e quindi di pertinenza del medico, eliminando così la discrezionalità presente invece nei casi sopra citati dei progetti regionali.

È evidente che quanto riportato non vuole essere una descrizione esaustiva dello stato dell'arte dei progetti di Fse, ma un'esemplificazione delle diverse «filosofie» che si stanno seguendo per la realizzazione del Fse stesso e dei problemi che ne sono connessi: naturalmente a fronte di differenti «filosofie» vi sono differenze in termini di obiettivi dello strumento, di dati, di loro semantica, di loro utilizzo (cioè, in buona sostanza, di aspetti applicativi) con conseguenti difficoltà e problemi sul piano della comunicazione dei dati a livello nazionale: l'enfasi posta su una finalità d'uso piuttosto che un'altra comporta inevitabilmente difformità sia nelle strutture dei dati sia nelle applicazioni che li utilizzano. L'aspetto che si sta discutendo è di estrema rilevanza, data la criticità dei dati in questione; si tratta della salute dei cittadini che, ad esempio, non sono obbligati ad ammalarsi nella regione di residenza: da questo punto di vista è essenziale garantire l'accesso ai dati sanitari da qualunque punto del pae-

[5] È opportuno ricordare, infatti, che il Servizio sanitario ha carattere nazionale e non regionale e pertanto il Fse deve necessariamente essere uno strumento a supporto della cura del cittadino che superi i confini territoriali e l'organizzazione delle strutture sanitarie e ospedaliere presenti in ciascuna regione.

se, tema che non pare dominare le «filosofie» dei vari progetti; si è portato un unico esempio, ma altri potrebbero essere citati (ad esempio il ruolo e le possibilità di intervenire sui dati da parte del singolo cittadino) ad esemplificare meglio le criticità dell'attuale situazione.

Gli esempi ed i dati riportati indicano chiaramente che il progetto di Fse, che il Ministero vorrebbe disponibile sull'intero territorio nazionale entro il 2012, non si sta sviluppando all'interno di una visione strategica unitaria e finalizzata a medesimi e univoci scopi, come altrettanto evidente è la mancanza di una regia operativa unica in grado di coordinare i vari progetti e di finalizzarli ad un unico obiettivo generale (banalmente garantendo, ad esempio, l'uguaglianza delle strutture dei dati e il loro valore semantico).

A fronte della situazione evidenziata sopra, vi è un aspetto ancora da puntualizzare: precisamente il costo che ha sostenuto e attualmente sta sostenendo il paese per l'implementazione di quanto sopra descritto, senza tuttavia che le strutture sanitarie, gli operatori e i cittadini possano usufruire dei vantaggi che la realizzazione del Fse comporterebbe: da questo punto di vista è evidente che la mancanza di un piano nazionale o per lo meno di una «regia» nazionale è un fattore di particolare criticità.

Data la disomogeneità delle situazioni nelle diverse regioni, il problema della stima dei costi sostenuti attualmente e nel passato nell'ambito del Fse si presenta piuttosto complesso; d'altro canto l'obiettivo che ci si propone è fornire degli strumenti di comparazione dei costi del Fse in determinate e note condizioni: a tale fine, per lo scenario in discussione, si sono considerate le diverse situazioni delle regioni in termini di differenti livelli di sviluppo del progetto, e si sono assunti valori medi di spesa in funzione delle diverse componenti del progetto e del diverso grado di sviluppo; i dati analitici sono stati raccolti e discussi con alcune regioni e alcune Asr e si è successivamente proceduto alla loro standardizzazione per poterli applicare alle diverse realtà regionali. Data la complessità dello specifico obiettivo e le finalità che ci si propone, si è preferito elaborare valori complessivi di massimo e di minimo, proprio come «indicatori» della spesa. Al fine della stima dei valori si è tenuto conto della realizzazione dei dossier clinico-sanitari nelle Asr, degli archivi

anagrafici degli assistiti piuttosto che degli operatori sanitari e dei servizi di interoperabilità per l'acquisizione delle informazioni dalle strutture sanitarie ove ci sono stati contatti di cura del paziente. Il perimetro di stima non comprende gli strumenti di identificazione e firma digitale per i professionisti sanitari e quelli per l'autenticazione informatica del cittadino, strumenti peraltro fondamentali in questo campo.

In queste ipotesi si stima che la spesa sostenuta dalle regioni italiane per l'implementazione di progetto di Fse, negli ultimi anni, si possa ritenere compresa tra i 670 e i 720 milioni di euro per lo sviluppo e tra i 130 e i 150 milioni di euro annui per la gestione e la manutenzione. A queste spese vanno aggiunti i costi che le regioni sostengono sotto forma di incentivi ai medici per il trattamento informatico dei dati sanitari e quelli sostenuti dai medici per la manutenzione delle loro dotazioni e per il collegamento di rete pari a circa 444 milioni di euro l'anno, come indicato nell'Appendice 1. Tutto ciò, come detto, senza i benefici attesi dal Fse.

3.3.3. Il modello proposto

Si sono assunte le seguenti ipotesi rivolte a definire un modello logico valido per tutto il territorio nazionale, indipendentemente da quanto possa essere stato realizzato o sia in fase di realizzazione presso specifiche regioni:

– per fascicolo sanitario elettronico si intende lo strumento che, attraverso un'architettura di interoperabilità e la cooperazione tra i sistemi informativi clinici delle Asr, mette a disposizione degli operatori sanitari e dei singolo cittadini la documentazione sintetica ed integrata, in formato digitale, relativa ai dati sanitari e socio-sanitari derivanti dagli eventi clinici avvenuti durante la vita del singolo cittadino;

– secondo quanto stabilito dalla normativa, le informazioni ed i dati clinici del singolo cittadino sono conservati esclusivamente presso l'ente dove sono stati prodotti nel dossier[6] clinico-sanitario:

[6] Il concetto di dossier presente all'interno di ciascun dominio delle Asr si rende necessario per evitare che il Fse debba acquisire dati e documenti da ciascun applicativo software.

il Fse non è quindi il risultato dell'aggregazione dei dati in un unico archivio elettronico, ma un insieme di servizi Ict che consentono ad un operatore sanitario debitamente autorizzato di accedere ai dati clinici di un paziente ovunque questi siano conservati e ovunque lui si trovi;

– che ciascuna regione si doti di una rete per la sanità alla quale possano accedere solo i soggetti autorizzati ad usufruire del servizio di Fse: la rete garantisce la possibilità di comunicare tra le Asr della regione di appartenenza e delle altre regioni per la realizzazione del fascicolo su tutto il territorio nazionale. Inoltre il «dominio» (insieme delle infrastrutture tecnologiche, dati e procedure informatiche che da un punto di vista legale afferiscono ad un determinato soggetto giuridico titolare della sicurezza) di ogni regione detiene i dati anagrafici degli assistiti (integrando quelli delle Asr), degli operatori sanitari e delle strutture sanitarie;

– che ciascuna regione istituisca un Centro tecnico[7], quale terza parte fidata degli enti sanitari, a cui venga affidata la gestione dei servizi della rete della sanità e vengano assegnate le relative risorse economiche necessarie al suo funzionamento; il Centro tecnico è pertanto uno strumento istituzionale ed organizzativo di governo, monitoraggio e sviluppo del sistema nel suo complesso; i costi dell'implementazione di tale struttura non vengono considerati nel seguito, in quanto potrebbe anche essere utilizzata una struttura già esistente, che è presente praticamente in tutte le regioni;

– nel modello che si utilizzerà non vengono considerate le strutture sanitarie convenzionate e/o private accreditate presenti nelle singole regioni. Qualora fosse d'interesse si possono estendere le stime calcolare per le Asr anche a queste strutture;

– Mmg/Pls sono considerati utenti afferenti ad una Asl e pertanto le ricette e il *patient summary* sono considerati documenti elettronici presenti all'interno del dominio dell'azienda di riferimento.

[7] A questo scopo andrebbe modificata la «legge Bersani» per consentire ai centri tecnici di poter agire in nome e per conto di più regioni. In questo modo si potrebbero realizzare importanti economie di scala nella realizzazione del Fse.

In sintesi si può affermare che il modello di Fse descritto si basa sul concetto d'interoperabilità, cioè sulla capacità di un sistema informativo di interagire con altri sistemi informativi in modo trasparente per l'utilizzatore e indipendentemente dalle tecnologie utilizzate per la loro realizzazione; ciò in quanto l'interoperabilità tra i servizi e la condivisione di documenti e informazioni si sostanzia nella possibilità da parte di un operatore sanitario, indipendentemente da dove si trovi la sua postazione di lavoro, di accedere, in modo efficiente e controllato, a tutte le informazione sanitarie di un paziente, indipendentemente da dove queste siamo conservate, attraverso la collaborazione con tutti i sistemi informativi clinici delle Asr. Il modello architetturale sottostante si basa su un insieme di domini relativi a soggetti giuridici differenti (aziende ospedaliere, aziende sanitarie, regione, ecc.) ciascuna titolare della sicurezza e responsabile della *privacy* secondo le disposizioni di legge vigenti (d.lgs. 30 giugno 2003, n. 196).

I domini coinvolti per ogni regione sono pertanto i seguenti:

– Asl e Ao: sono i domini di una generica azienda sanitario locale od ospedaliera responsabile della raccolta e della conservazione delle informazioni clinico-sanitarie (costituente il dossier sanitario) e dell'implementazione delle *policy* per l'accesso alle informazioni; in questi domini sono gestiti gli archivi locali dagli assistiti (Ala). I documenti elettronici presenti nei dossier sono firmati digitalmente[8] dai professionisti sanitari che li hanno prodotti. I dossier contengono anche le ricette e il *patient summary* prodotti da Mmg/Pls nelle Asl di loro appartenenza;

– Centro tecnico: è il dominio terzo che eroga i servizi necessari all'integrazione, che deve pertanto garantire la sicurezza, l'affidabilità, il tracciamento e il monitoraggio delle comunicazioni, l'instradamento delle richieste e i servizi di autenticazione e autorizzazione degli attori del sistema;

– Regione: è il dominio in cui risiedono i sistemi informativi del-

[8] Necessaria l'adozione della firma digitale affinché il documento elettronico si possa considerare sostitutivo di quello cartaceo (come previsto dal Codice dell'amministrazione digitale).

l'ente regionale, in particolare le anagrafiche di riferimento: nel dominio regione vengono pertanto gestiti l'archivio regionale degli assistiti (Ara), l'archivio degli operatori sanitari (Aos) e l'anagrafica delle strutture sanitarie[9].

3.3.4. Lo scenario conservativo

3.3.4.1. I costi di implementazione

A seguito dell'attività di confronto e raccolta dati con alcune regioni e Asr, come detto nel paragrafo 3.3.1, per la definizione dei costi unitari si è pervenuti alle seguenti ipotesi:

– che la costituzione dei Fse avvenga per regione, conservando l'approccio attuale che vede appunto ogni regione intervenire autonomamente;

– che per ogni regione si spendano 3.800.000 euro per la realizzazione della rete della sanità (inclusi i costi di infrastruttura e dei servizi software di interoperabilità ed i costi per l'implementazione del servizio di gestione del consenso del cittadino al Fse) e 1.100.000 euro per i costi di collegamento tra le singole aziende e la rete;

– che a livello regionale, per l'implementazione degli archivi precedentemente indicati, vengano mediamente spesi per ogni cittadino:

– 0,36 euro, per gli archivi Ara,

– 0,19 euro, per gli archivi Aos,

includendo l'attività di controllo qualità dei dati anagrafici e delle eventuali bonifiche da parte delle Asr;

– che per ogni Asr, vengano mediamente spesi:

– 970.000 euro, per software applicativo, d'ambiente e servizi d'installazione, assistenza, personalizzazione e integrazione con altro software presente (ad esempio quello degli strumenti tecnico-sanitari) per l'implementazione dei dossier clinico-sanitari;

– 1.100.000 euro, per l'adeguamento della rete interna e le relative dotazioni hardware, inclusi i collegamenti ridondati per garantire alta affidabilità;

– 650.000 euro, per le infrastrutture hardware di calcolo, incluso le infrastrutture ridondate per garantire il *disaster recovery*;

– 540.000 euro per la realizzazione degli archivi Ala;

– sempre per ogni Asr, una spesa di particolare rilievo è costituita da quella derivante dalle attività di adeguamento dei software dell'area clinica all'autenticazione e alla firma digitale; la stima del costo di questa operazione è piuttosto complessa data l'estrema eterogeneità dei software installati: infatti, secondo stime compiute in alcune regioni, il numero complessivo di pacchetti installati presso le aree cliniche delle Asr di una regione varia da 700 a 780, inoltre non sono sempre uguali per una determinata area clinica. Presso alcune Asr tuttavia l'attività di adeguamento è stata effettuata su alcune applicazioni dell'area clinica: alla luce di queste esperienze e dei relativi costi si è pervenuti a stimare in 2.700.000 euro la spesa media per Asr per questa attività; il valore assunto come stima è comunque prudenziale, data la mancanza di dati completi sui costi di adeguamento per tutte le differenti applicazioni installate: infatti non solo vi è differenza tra le applicazioni cliniche, ma vi è differenza anche tra le diverse soluzioni dei diversi fornitori per la medesima area. Data la finalità del documento si è ritenuto comunque utile fornire una valutazione anche di questa voce di spesa, al fine di disporre di un quadro più completo.

– non vengono considerati i costi per dotare gli operatori sanitari, inclusi Mmg e Pls, degli strumenti di firma digitale;

– si è ipotizzato di definire contrattualmente, con i fornitori dei software clinici, che le attività di adeguamento dei software installati in un numero elevato di copie nelle differenti Asr venga pagato una sola volta e che quindi venga reinstallato il software modificato in tutte la realtà che ne sono dotate.

Alla luce delle ipotesi indicate, i costi stimati per l'implementazione del progetto sono risultati pari a 1.987 milioni di euro, come indicato in dettaglio nell'Appendice 2.

[9] Nel modello consideriamo che ciascuna regione sia già dotata di una anagrafica strutture.

3.3.4.2. Costi annui di gestione e manutenzione

Per la raccolta dei dati economici di riferimento si è proceduto, come nel precedente caso, raccogliendo informazioni e dati reali presso regioni che hanno allo studio o stanno implementando progetti di Fse e presso alcune Asr; anche in questo caso i dati raccolti sono stati normalizzati e generalizzati a tutte le realtà regionali e a tutte la Asr.

I dati raccolti, sempre in relazione alle aree cliniche, hanno riguardato le seguenti voci e i rispettivi valori di spesa per la quota parte relativa alle attività di gestione e manutenzione:

– personale interno ed esterno,
– hardware,
– software,
– noleggi,
– energia elettrica

e tutte le altre spese, in quota parte, sempre riconducibili alle attività di gestione e manutenzione delle aree precedentemente indicate.

Ciò ha permesso di definire in 3.800.000 euro la spesa media annua di un'azienda per le attività qui considerate, vale a dire quelle relative alle sole aree cliniche.

Per quanto riguarda la stima delle spese di gestione e manutenzione del progetto per la realizzazione del fascicolo, come sopra definito, si è convenuto nello stimare tale valore nel 20% dei costi sostenuti (anche questo valore su base annua).

Per quanto riguarda i medici è stata stimata pari a 2.600 euro il costo medio annuo che ogni Mmg/Pls deve sostenere per la gestione e la manutenzione del software e dell'hardware e per il collegamento di rete necessario: si tratta quindi delle spese che il medico, oltre al collegamento di rete, deve sostenere per dotarsi di pc (di cui vengono considerati gli ammortamenti), software, stampante e materiale di consumo. A questi costi, comunque sostenuti dai medici ma che in ogni caso concorrono alla formazione delle spesa totale che il sistema sanitario deve sostenere, occorre aggiungere gli incentivi, che si configurano come veri e propri costi di gestione, che le regioni riconoscono ai medici di base per il trattamento dei dati sanitari in formato elettronico, stimati in 5 euro per paziente all'anno.

Alla luce delle ipotesi precedenti i costi di gestione e manutenzione del progetto su base annua sono risultati pari a 1.852 milioni di euro, come indicati nell'Appendice 2.

3.3.5. Scenario evolutivo

Le analisi svolte hanno portato alla definizione di un secondo scenario. Come detto in precedenza i dati e i documenti elettronici relativi ai contatti di cura dei pazienti con le Asr sono conservati all'interno dei dossier di competenza del dominio dell'ente. Il fascicolo, attraverso i servizi di interoperabilità della rete della sanità, è in grado di reperire la documentazione clinica presente nei dossier allo scopo di offrire un quadro sintetico e unitario della storia clinica del paziente. Il contenuto informativo dei dossier è prodotto dagli applicativi software presenti nel sistema informativo clinico-ospedaliero delle Asr (ad esempio la lettera di dimissione dal software Adt, il referto di una visita specialistica dalla cartella clinica, ecc.).

Lo stato dell'arte dei software dell'area clinica delle Asr risulta in larga misura obsoleto e caratterizzato da:

– significativa ridondanza dal punto di vista della copertura funzionale (diversi prodotti per le medesime esigenze di informatizzazione);
– elevata eterogeneità tecnologica;
– scarsa integrazione tra le applicazioni.

Come già detto, secondo stime compiute in alcune regioni, il numero di differenti software dell'area clinica installati presso le Asr varia da 700 a 780.

A questo proposito si possono fare alcune considerazioni: questa estrema frammentazione richiede una quota significativa delle spese di implementazione, indicate nello scenario conservativo, per rendere «compatibili» le applicazioni, spesa che sarebbe di adeguamento, non certo di tipo evolutivo; inoltre la frammentazione di cui si discute rende quasi impossibili qualunque ricorso all'utilizzo di servizi *cloud*, notoriamente basati sul principio della standardizzazione delle applicazioni utilizzate e rese disponibili.

Lo scenario evolutivo proposto si basa sull'ipotesi di realizzare

un'unica Piattaforma di sanità elettronica (Pse)[10] per l'automazione delle attività cliniche per tutte le Asr.

Il perimetro della Pse dovrebbe comprendere:

– anagrafe locale assistiti
– cup
– pronto soccorso
– accettazione, dimissioni, trasferimento
– blocco operatorio
– cartelle clinica infermieristica
– cartella clinica medica
– dossier sanitario

Si disporrebbe così di una piattaforma standard e in queste condizioni si potrebbe adottare una soluzione basata su servizi *cloud*, forniti da un numero limitato di soggetti, se non addirittura da un unico soggetto a livello nazionale.

In questo scenario si possono azzerare alcuni costi evidenziati in precedenza quali ad esempio la realizzazione degli archivi locali (Ala) e del dossier, in quanto già presenti all'interno della piattaforma Pse. Inoltre non sarebbe più necessario investire nell'adeguamento dei software delle Asr per l'autenticazione e la firma digitale poiché tali caratteristiche sarebbero previste all'interno della Pse.

Il perimetro della Pse non include i software di diagnostica ovvero:

– laboratorio analisi
– anatomia patologica
– radiologia
– trasfusionale

Per queste aree l'ipotesi è che ciascuna regione in accordo con le Asr scelga la soluzione «prevalente» ovvero quella che allo stato dell'arte risulta essere la più diffusa sul territorio regionale. Sulla base

[10] L'ipotesi è di acquisire la piattaforma attraverso una gara nazionale per tutte le Asr italiane.

di questa soluzione le regioni[11] in accordo con le Asr potrebbero sviluppare servizi su scala territoriale allo scopo di razionalizzare le risorse (ad esempio la costituzione di laboratori «logici» unici di area e /o regionali) e ridurre la ridondanza dei software oggi utilizzati e poter utilizzare anche per queste aree soluzioni in *cloud*.

Per quanto concerne i Mmg ed i Pls l'ipotesi è di dotarli di una soluzione di cartella clinica unica integrata con il Fse e con i servizi di Inps e Ministero dell'economia per la trasmissione rispettivamente dei certificati di malattia e delle prescrizioni elettroniche. Oltre ai benefici indotti sull'operatività del medico e del cittadino (ad esempio il medico potrebbe consultare attraverso il Fse un referto di un esame da lui richiesto) si potrebbe raggiungere significative economie di scala grazie all'introduzione di un servizio comune, per altro erogabile tramite soluzioni in *cloud computing*.

In questo scenario si può inoltre considerare l'azzeramento dell'incentivo, oggi richiesto dai Mmg e dai Pls, per il trattamento dei dati elettronici dei loro pazienti: la possibilità di erogare un servizio unico su scala nazionale consentirebbe di liberare risorse specializzate che potrebbero essere utilizzate per offrire agli studi medici tutto il supporto tecnico necessario tramite call center e/o interventi diretti, necessità cui oggi devono far fronte in modo autonomo, con tutte le difficoltà che questo comporta e che vengono «compensate» sul piano economico degli incentivi di cui sopra.

3.3.5.1. Costi di implementazione

Sulla base delle considerazioni precedenti, e secondo il metodo già indicato, si sono effettuate delle stime di costo per l'implementazione del progetto e precisamente:

– 1.100.000 € per ogni Asr come quota parte delle spese per l'implementazione della piattaforma unica;

– 4.350.000 € per ogni Asr per le spese per la sostituzione dei software presenti nel perimetro della Pse (vedi sopra);

[11] In questo scenario al momento non sono state valutate le possibili ulteriori razionalizzazioni e di conseguenza risparmi indotti dalla presenza dello stesso fornitore su più regioni.

– 5.000.000 € per ogni Asr per le spese di sostituzione e d'integrazione con la Pse dei software di diagnostica: laboratori analisi, radiologia, anatomia patologica, trasfusionale.

– 8.000.000 € per regione per l'impianto della soluzione unica di cartella per i Mmg e i Pls;

– 1.800 € per singolo Mmg/Pls per la dotazione del software e dell'hardware necessario al collegamento con il Fse e di tutto il supporto necessario agli studi medici.

Come detto a questi costi vanno aggiunti quelli relativi all'implementazione degli archivi regionali degli assistiti (Ara) e degli operatori sanitari (Aos), i costi di adeguamento della rete interna delle Asr le relative dotazioni hardware inclusi i collegamenti ridondati (1.100.000 € per Asr) ed i costi relativi all'implementazione della rete della sanità e al collegamento di rete tra la rete e le Asr, già stimati in precedenza.

Nelle ipotesi indicate i costi d'implementazione risultano pari a 3.732 milioni di €, come indicato nell'Appendice 2.

3.3.5.2. Costi annui di gestione e manutenzione

Data le caratteristiche dell'architettura dello scenario in considerazione, tra queste spese non figurano i 3.500.000 € per Asr dovute alla gestione delle rispettive aree cliniche; analogamente a quanto definito nello scenario conservativo, per queste spese si può assumere, su base annua, il 20% del costo totale del progetto che risultano pari a 746 milioni di euro, come indicato nell'Appendice 2.

3.3.6 Confronto tra i costi degli scenari

Sulla base delle ipotesi adottate, i costi totali per dotare tutti i cittadini italiani del Fse sono sintetizzati nella seguente tabella.

Tabella 2. Costi per dotare tutti i cittadini di Fse

	Implementazione	Gestione
Scenario Conservativo	€ 1.987.778.000	€ 1.852.814.600
Scenario Evolutivo	€ 3.732.471.000	€ 746.492.000
Delta	-€ 1.744.693.000	€ 1.106.322.600

Lo scenario evolutivo presenta una spesa d'implementazione pari a circa 1,9 volte quella dello scenario conservativo, ma una spesa per gestione e manutenzione, e quindi ricorrente, pari a circa il 40% di quella dello scenario conservativo. Di particolare interesse risulta l'evoluzione del delta di spesa; infatti proiettati i dati su un arco di medio lungo periodo, su cinque anni, si ottiene il seguente scenario.

Tabella 3. Costi per dotare tutti i cittadini di Fse per gestione su 5 anni

	Implementazione	Gestione sui 5 anni	
Scenario Conservativo	€ 1.987.778.000	€ 9.264.073.000	
Scenario Evolutivo	€ 3.732.471.000	€ 3.732.460.000	
Delta	-€ 1.744.693.000	€ 5.531.613.000	
Riduzione della Spesa			€ 3.786.920.000

Pur nelle semplificazioni e schematizzazioni dichiarate all'inizio, che sono conseguenti all'attività di modellazione che è alla base di questa analisi, si può ritenere che sulla base del modello definito la soluzione basata su servizi *cloud* permetterebbe un risparmio, nell'arco di 5 anni, di oltre 3,7 miliardi di euro.

3.4. La ricetta elettronica

A causa delle possibili sinergie con il Fse, si accenna nel seguito al tema della ricetta elettronica: è infatti utile analizzare brevemente il tema in quanto la realizzazione del Fse costituirebbe un fattore abilitante ulteriori risparmi di spesa, nello specifico di spesa sanitaria, in associazione con la ricetta elettronica.

Alcune regioni hanno avviato progetti di ricetta elettronica nell'ottica della piena smaterializzazione della ricetta stessa, senza tuttavia arrivare alla conclusione dei progetti e alla piena operatività delle soluzioni tecnologiche. Le ragioni sono molteplici, ma soprattutto sono da ricondurre a visioni parziali e non integrate del progetto: in particolare il Ministero dell'economia ha dato un significativo impulso al progetto, ma in un'ottica puramente finanziaria, nella prospettiva del controllo della spesa sanitaria, obbligando i medici ad inviare il prescritto in formato elettronico (oggi i dati sull'erogato vengono forniti al Ministero dalle regioni su supporto elettronico[12] a cadenza mensile).

Va tuttavia tenuto presente che l'acquisizione di questi dati finalizzati, come detto, al controllo della spesa, non consente di raggiungere la piena digitalizzazione della ricetta: come noto, nel caso delle prescrizioni farmaceutiche, le farmacie oggi appongono l'etichetta adesiva (detta «fustella») sulla copia cartacea della ricetta al momento della consegna dei farmaci al paziente; questa operazione, purtroppo, al momento non è gestibile elettronicamente in quanto il progetto «tracciabilità del farmaco» del Ministero della salute, che ha l'obiettivo di gestire la confezione del farmaco a partire dal momento in cui viene messo in commercio fino all'erogazione al paziente, non è stato ancora del tutto avviato.

In questa situazione alcune regioni hanno comunque avviato il progetto di ricetta elettronica, ritenendo di ovviare a questa lacuna col chiedere alle farmacie di conservare un registro cartaceo sul quale annotare le fustelle. A questo si aggiunge la considerazione che gli applicativi software in uso presso le farmacie sono, tanto per cambiare, differenti e, spesso, a causa della loro obsolescenza tecnologica, non facilmente integrabili con servizi *web*.

La dotazione alle farmacie, come ai medici di base, di un servizio in *cloud* basato su un software unico collegato alla banca dati del Ministero della salute (detta anche banca dati dei bollini unici) e al Fse consentirebbe di raggiungere la piena smaterializzazione della ricetta elettronica e di controllare il dato della spesa nazionale farmaceutica in tempo reale.

Infine occorre considerare anche le ricette «bianche», prodotte all'interno delle strutture ospedaliere che, grazie alla dotazione di una piattaforma unica di sanità elettronica, potrebbero essere più facilmente rese disponibili attraverso il Fse e così contribuire a completare il quadro complessivo per quanto concerne il consumo di farmaci. Al contrario oggi la dotazione di molteplici strumenti presenti all'interno dei sistemi informativi ospedalieri complica ulteriormente la possibilità di acquisire tali informazioni.

I risparmi stimati con la smaterializzazione della ricetta «rossa» ammontano, secondo una stima del Ministero della salute, a circa 5 miliardi di euro all'anno.

È evidente che un investimento importante si giustifica anche sotto il profilo della sostenibilità economica, in quanto i significativi risparmi indotti dalla sola smaterializzazione della ricetta consentirebbero di raggiungere in un tempo ragionevole (4-5 anni) il *break-even*.

Senza dimenticare gli ulteriori benefici, al momento non quantificabili, collegati ad una inutile o non corretta somministrazione di farmaci, ai rischi che questo comporta per i pazienti e agli eventuali ulteriori costi indotti da errori dei professionisti causa mancanza di informazioni.

4. Il Comune

4.1 Gli schemi organizzativi

Nel seguito vengono presentati alcuni schemi relativi alla fase di «scomposizione» delle attività del comune: senza avere la pretesa dell'esaustività bensì, come detto, di esemplificazione dei risultati dell'applicazione del metodo esposto.

[12] Flussi con elaborazioni di tipo *batch*.

Figura 6. Comuni – Ambito di destinazione: cittadini

Missione

Il comune governa un sistema complesso di entità e di relazioni che ha, come obiettivo principale, di garantire lo sviluppo e la tutela della qualità della vita dei cittadini, intesi sia individualmente sia in associazione con altri, in collettività o nuclei, del territorio e dell'ambito produttivo che insiste sul territorio di competenza. Gestisce il sistema dei valori rivolto al miglioramento delle condizioni di vita dei cittadini, nelle sue molteplici forme, all'interno del quale definisce gli obiettivi che vuole perseguire e, conseguentemente, i servizi da fornire e le regole condivise che devono governare il sistema di relazioni sociali e territoriali. Ha quindi due centri di riferimento tra loro correlati: il cittadino ed il territorio, per i quali studia e realizza servizi rivolti al raggiungimento degli obiettivi indicati in precedenza.

Cardini

Regole

Il procedimento amministrativo è il fulcro dell'attività del comune e si realizza attraverso un sistema di regole articolato su più livelli (sistema delle fonti) che vede presenti:

Quest'ultima è di particolare rilevanza in questa sede in quanto, tra gli altri aspetti, data la massima vicinanza dell'ente regolamentante al territorio che deve "gestire",
è una delle fonti delle differenze riscontrabili nella prassi tra comune e comune, e tra comuni di regioni diverse, causa l'azione della legislazione regionale che porta a "riflettere" le proprie direttive nella produzione regolamentare locale. Gli atti amministrativi (cioè gli atti giuridici posti in essere da un'autorità amministrativa nell'esercizio delle sue funzioni e che producono effetto nei confronti dei soggetti cui sono rivolti, indipendentemente dalla loro volontà) propri dei comuni sono:

– autorizzazioni,
– concessioni,
– licenze.

Va in particolare osservato che i regolamenti dettagliano, all'interno delle legislazione nazionale e regionale, l'insieme delle regole minime che devono disciplinare i comportamenti, secondo le peculiarità della specifica realtà sociale e territoriale; d'altro canto gli atti consigliari o della giunta (quindi a valenza politica) hanno un carattere di indirizzo, di individuazione degli obiettivi, in un certo senso strategici, mentre quelli dirigenziali hanno un carattere operativo, fornendo indicazioni su come eseguire il deliberato politico.

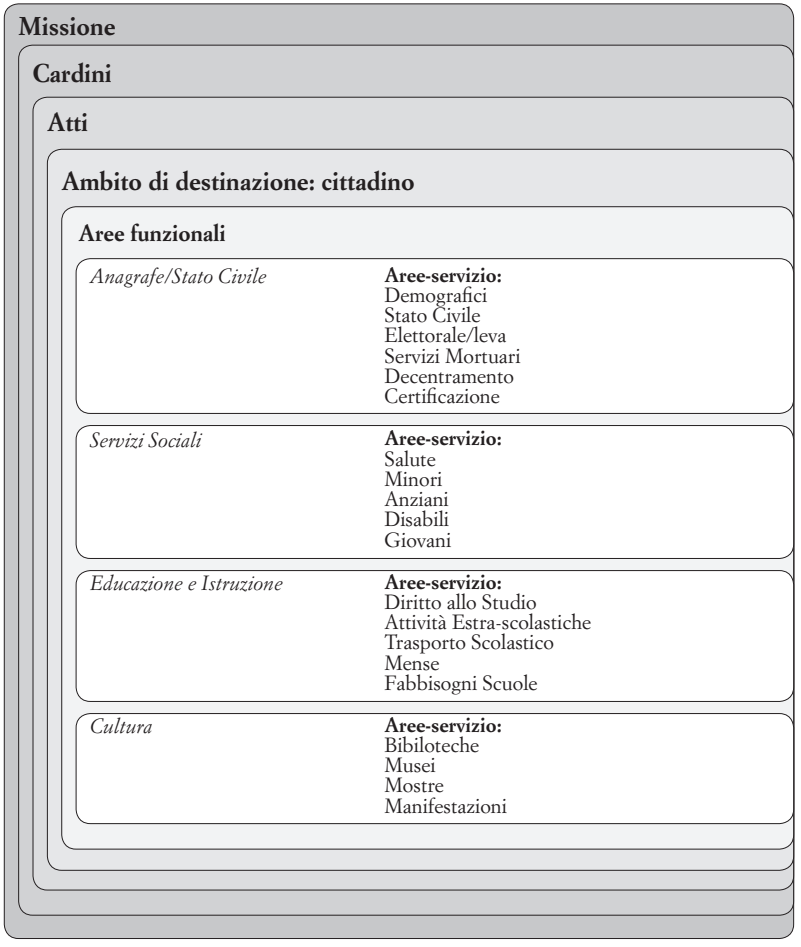


Figura 7. Ambito territorio

Missione

Cardini

Atti

Ambito di destinazione: territorio

Aree funzionali

Sicurezza e Polizia municipale	**Aree-servizio:** Vigilanza urbana e Presidio del Territorio Polizia Giudiziaria Protezione Civile
Trasporti Locali e Mobilità	**Aree-servizio:** Pianificazione Mobilità Pianificazione Viabilità Pianificazione Soste e Parcheggi Pianificazione Traffico Pianificazione Trasporti
Attività Produttive	**Aree-servizio:** Sportello Unico A.P. Coordinamento Enti esterni Gestione Attività Commerciali Programmazione Rete Distributiva Osservatorio del Mercato del Lavoro Sviluppo Occupazione Piani Formazione Orientamento e inserimento del Lavoro
Edilizia Pubblica	**Aree-servizio:** Immobili Pubblici
Edilizia Privata	**Aree-servizio:** Gestione Domande di Costruzione Rilascio Permessi Controllo Interventi Privati Gestione Sanzioni Gestione Contenzioso Catasto
Urbanistica	**Aree-servizio:** Piano del Governo del Territorio Varianti di Piano Piani Integrati di Intervento Sistema Informativo Territoriale
Lavori Pubblici	**Aree-servizio:** Strade Unfrastrutture Immobili Pubblici Opere di Urbanizzazione
Patrimonio	**Aree-servizio:** Patrimonio Mobiliare Patrimonio Immobiliare

Figura 8. Ambito Ente comunale

Missione

Cardini

Mezzi

Ambito di destinazione: Ente Comunale

Aree funzionali

Area Economico/Finanziaria	**Aree-servizio:** Ministero Economia CDDPP Sistema Bancario Sistema Assicurativo Tesoreria Esattoria Cittadini Aziende Private Società Partecipate
Area Personale	**Aree-servizio:** Ministero Funzione Pubblica Sistema Previdenziale Sistema Sanitario Locale Enti Locali Università/Scuole Superiori Dipendenti Ispettorato del Lavoro Organizzazioni Sindacali Agenzia Entrate/CAF Tribunali/Prefetture Aziende Private

Prima di procedere alla definizione dello schema delle relazioni del comune o, meglio, delle relazioni delle sue componenti funzionali tra loro e con altri enti, occorre fare alcune considerazioni sul livello operativo o strategico delle sue attività, dei suoi «atti»; il tema è abbastanza complesso in quanto si tratta di attribuire una connotazione precisa e non ambigua al «significato» di una determinata azione dell'ente. Non vi è dubbio che la produzione di un certificato vada considerata attività operativa, in quanto la produzione del certificato non persegue fini di altro ordine, si esaurisce in se stessa, anche se lo specifico certificato va ad integrare un'altra pratica, contribuendo a completarla; d'altra parte è indiscutibile che un atto come la stesura del Piano di governo del territorio abbia valenza stra-

tegica, in quanto definisce le regole, le funzioni d'uso e la rete dei servizi del territorio per gli anni successivi, definendone quindi il futuro sviluppo, secondo quanto impone la missione del comune; più complesso è dare un attributo di questo tipo, ad esempio, ai servizi di assistenza agli anziani o di gestione di una biblioteca; in questi casi il servizio, pur se si esaurisce nel momento della sua fornitura, ha un «secondo fine», tende al raggiungimento di un obiettivo di altro ordine: rispondendo alla missione del comune, contribuisce al miglioramento, rispettivamente, del benessere dell'anziano o della cultura del cittadino che si reca in biblioteca, entrambi obiettivi strategici. Vi è comunque un altro fattore per categorizzare le azioni di un comune: la questione delle risorse finanziarie; si vuole dire che, a parte alcune attività che hanno, per il comune, una connotazione di obbligatorietà (ad esempio la gestione dell'anagrafe e dello stato civile), tutte le altre attività non hanno sostanzialmente tale connotazione, in quanto la loro realizzazione è strettamente dipendente dalla disponibilità delle relative risorse finanziarie; in questo contesto vi sono in particolare due fasi a monte dell'erogazione del servizio: in un primo momento vi è la scelta, da parte dello stato, almeno sino ad approvazione di differenti leggi connesse al processo di implementazione del federalismo, dell'ammontare complessivo delle risorse finanziarie che vengono trasferite ai comuni ed al singolo comune e, successivamente, vi è la scelta, da pare del comune, di come allocare tali risorse: in entrambi i momenti si tratta di una scelta «strategica» e quindi in sostanza politica. La scelta delle attività cui destinare le risorse finanziarie, la quantificazione e distribuzione delle medesime ha quindi una valenza politica, che informa di tale carattere anche i servizi che di conseguenza vengono erogati. D'altronde il tema è di grande attualità: lo stato di crisi economica che il paese attraversa sta comportando la riduzione delle risorse finanziarie disponibili per i comuni, ma non solo, e questi, a loro volta, si vedono costretti a operare delle scelte, riducendo determinati servizi piuttosto che altri. Se la decisione di finanziare un determinato servizio è strategica, altrettanto lo è la sua erogazione, in quanto risponde ad un obiettivo di ordine superiore. Sia pure con qualche semplificazione, si possono quindi considerare operativi i soli servizi di certificazione dell'anagrafe, dello stato civile e simili, e

strategici gli altri.

Per quanto riguarda il modello che si sta discutendo ciò, comunque, non pone differenze dal punto di vista dell'analisi da svolgere: si tratta di una caratteristica aggiuntiva che qualifica la specifica azione del comune ed è utile all'attività di «ricomposizione» cui si è accennato in precedenza che porta alla definizione dei processi; si consideri a questo proposito l'estrema varietà dei motivi per cui un cittadino, in forma singola o aggregata, ha interazioni con il comune e le sue strutture funzionali e di come queste rispondono: il cittadino può avere necessità di un certificato anagrafico (che può essere un elemento di un processo più ampio che coinvolge altri enti, ma di cui il comune non ha responsabilità; può voler vedere una mostra o chiedere un libro in prestito alla biblioteca (ed in realtà non si domanda se stia o meno interagendo con il comune, ma bensì si limita a «fruire» di un servizio che, sostanzialmente, ritiene venga erogato dalla struttura che gli è di fronte, museo o biblioteca che sia); può avere bisogno di assistenza sociale (ed allora, data la sua posizione di «bisognoso di assistenza» si aspetta un determinato tipo di attenzione o comunque di capacità nel risolvere i propri problemi, senza che lui stesso venga coinvolto in ruoli supplenti le attività attese dal comune); ha necessità di una licenza (ed è rassegnato a svolgere la funzione di «portalettere» tra gli uffici comunali per portare da un ufficio all'altro documenti che il comune già possiede): la ragione di questi esempi è semplice. Si è detto prima del carattere operativo o strategico/politico delle attività del comune che tuttavia, nella prassi, perdono completamente tale carattere e confermano la concezione segmentata delle attività delle unità funzionali degli enti: gli esempi sono sostanzialmente un altro modo di presentare le criticità indicate in precedenza che, se superate, permetterebbero di raggiungere sicuramente maggior efficacia nell'azione del comune e maggior soddisfazione nei cittadini.

4.2. Gli schemi generali dei flussi

La rappresentazione che segue è sintetica e, per certi versi, anche incompleta; è tuttavia importante perché rende evidenti due fattori decisivi:

– ciò che è chiamato «relazione stato/luogo»;
– il ruolo del protocollo.

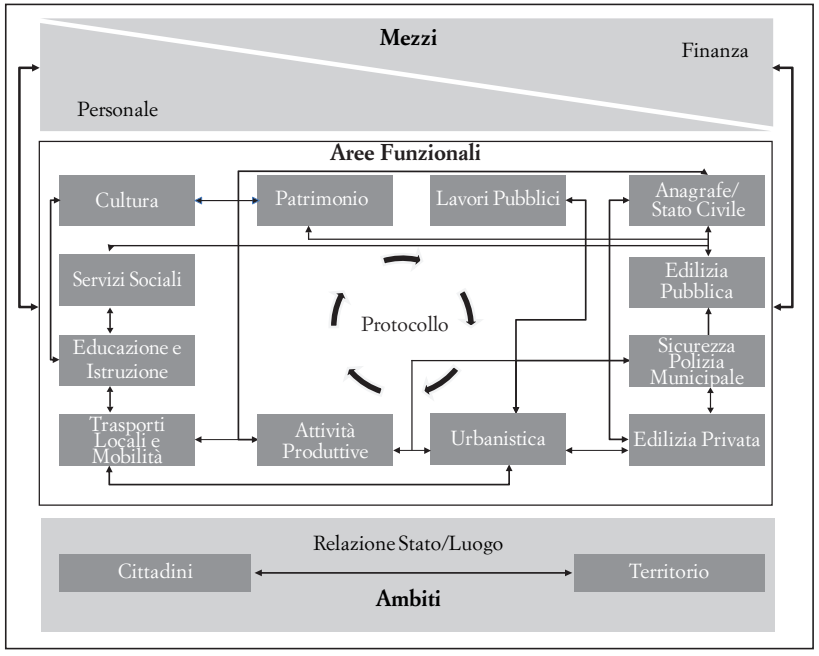
Al fine della riorganizzazione delle attività per processi, il primo fattore è fondamentale: se si riflette sulle relazioni tra cittadini e territorio si osserva che tra le entità che compongono le due categorie esiste un insieme preciso di relazioni; il rapporto del cittadino con il territorio non si esaurisce con l'indirizzo: il cittadino, infatti, non solo risiede in un determinato «luogo fisico» con un preciso indirizzo, ma ha con il territorio un rapporto che varia e si modifica negli anni, al variare del suo «stato»: va ad un asilo, va ad una scuola, lavora in una azienda, ha una macchina, si diverte, apre un'attività commerciale o da vita ad un'iniziativa imprenditoriale, inquina il territorio, lo sfrutta in modo scorretto o ne occupa abusivamente una parte; in altre parole il cittadino modifica continuamente la relazione tra se e i «luoghi fisici» che lo riguardano o lo interessano. Si considerino ora i cittadini, i singoli cittadini, e il territorio, cioè la sua struttura, le sue caratteristiche e le sue destinazioni d'uso, come degli archivi di dati che li «descrivono», come in realtà sono: abitualmente vengono considerati e costituiti in archivi distinti e non comunicanti, mentre si è visto come le loro componenti, lo «stato» del cittadino e i «luoghi fisici» con le loro caratteristiche, hanno un vero e proprio sistema di relazioni. Allo stato attuale i due archivi, in qualunque sistema informativo comunale, vivono di vita propria, con tutta una serie di conseguenze negative, dalla duplicazione dei dati, con altissimi tassi di errore, alla incapacità o impossibilità a fornire servizi efficienti; una visione integrata delle attività porta alla necessità di disporre, per prima cosa, di un archivio integrato cittadini-territorio che contenga, non solo i dati descrittivi delle entità ma anche, già codificate, le possibili relazioni tra gli elementi dell'uno e dell'altro, costituendo in tal modo uno strumento in grado di fornire «servizi» alle applicazioni che insistono su questi archivi, praticamente tutte la applicazioni di un comune.

D'altrettanta importanza è ciò che è stato indicato come «protocollo», termine che tuttavia da solo offre una visione limitata del problema che si vuole discutere. Considerando un comune si osserva che vi sono:

– flussi informativi che nascono all'esterno e che si esauriscono nel *front end* (il caso di emissione un certificato anagrafico), che in realtà fanno parte di servizi in cui non viene attivato alcun procedimento amministrativo;
– flussi informativi che nascono all'esterno e che vengono svolti e completati dalle unità funzionali dell'ente, spesso comportando il passaggio da un'unità organizzativa ad un'altra;
– flussi informativi che nascono all'interno dell'ente, da una determinata unità organizzativa e coinvolgono altre unità organizzative.

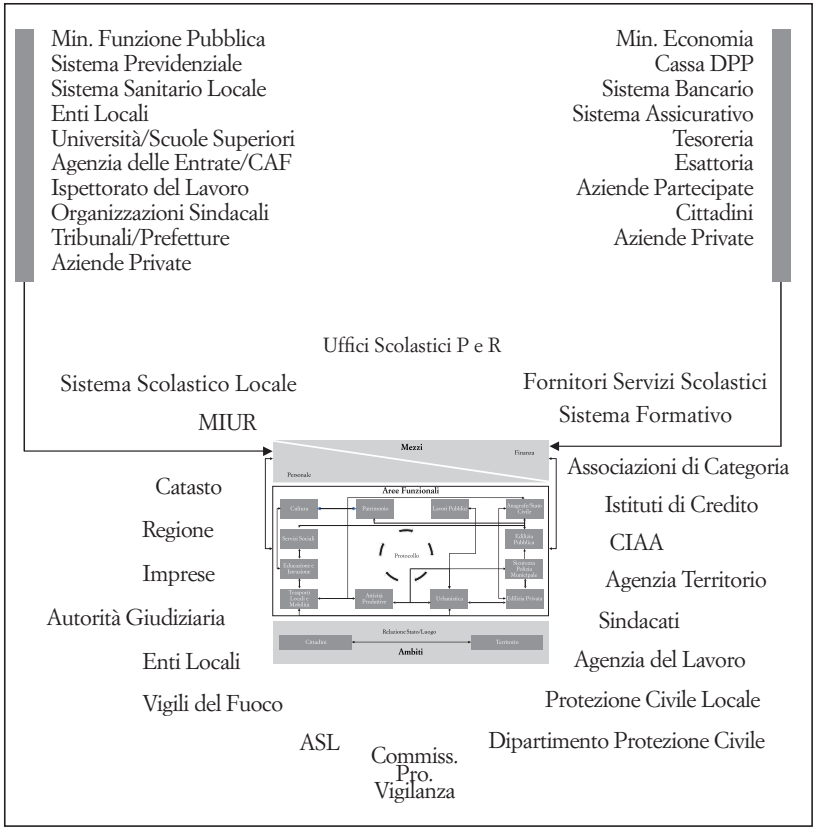
Solo per i secondi viene coinvolto il protocollo che, sulla base di una visione strettamente burocratica, si limita a seguire il processo innescato dall'arrivo di un determinato flusso informativo (documento), ma che potrebbe costituire la base per lo sviluppo di un sistema di comunicazione integrato dell'ente comunale: l'attività di un comune si esplica, per buona parte, nello svolgimento di procedimenti amministrativi che sono costituiti fondamentalmente da informazioni che vengono ricevute da una struttura, trattate e inviate ad un'altra struttura o, se terminate, al destinatario; le modalità di trasmissione delle informazioni, dal punto di vista dell'efficienza dell'ente e della possibilità, per il cittadino, di monitorarne le attività, rivestono un ruolo decisivo, ruolo che oggi è generalmente svolto manualmente. Ciò che l'analisi porta a concludere è la necessità di una infrastruttura di comunicazione che costituisca una sorta di «bus» in grado di fornire servizi comunicativi integrati a tutti gli elementi della struttura comunale: il protocollo può essere la base di tale sistema di comunicazione divenendo, da semplice sistema di registrazione dei documenti in ingresso, un sistema che, a partire da questo ruolo, «distribuisce» le informazioni nelle unità funzionali di destinazione e ne accompagna il percorso tra le eventuali altre unità sino al compimento del procedimento amministrativo aggregando i documenti ulteriori che via via vengono prodotti.

Figura 9. Mappa relazioni interne



Nel seguito si riporta lo schema generale delle relazioni del comune con gli enti esterni ad esso. La rappresentazione è svolta a un elevato livello di sintesi: lo schema completo dovrebbe indicare quale singola unità funzionale del comune è in relazione con quale singola unità funzionale di quale ente esterno, dettaglio descrittivo che esula dalle intenzioni del presente lavoro che intende essere, come detto, esemplificativo dell'applicazione del metodo descritto in precedenza; nel seguito si approfondiranno due casi particolari che verranno utilizzati per delineare gli schemi di possibili soluzioni in *cloud computing*

Figura 10. Mappa relazioni esterne



4.3. La situazione dei sistemi informativi e i costi

4.3.1. Lo scenario attuale

La situazione dei comuni è relativamente peculiare: sono infatti caratterizzati da identici compiti istituzionali, a partire dalla medesima base amministrativa, ma da significative differenze nelle modalità del loro svolgimento: le competenze sono infatti molto differenziate ed ampie, pur all'interno della stessa mappa funzionale, e le diversità sono dovute a due aspetti: da un lato le dimensioni (in termini di abitanti si va da alcuni milioni a poche centinaia) e le caratteri-

stiche, dall'altro la produzione legislativa. Con riferimento al primo aspetto va osservato che, se pur i compiti istituzionali sono i medesimi, le risorse finanziarie disponibili sono tendenzialmente proporzionali al numero di abitanti (quindi dai miliardi alle migliaia di euro) come anche i dipendenti (dalle decine di migliaia alle poche unità), ed è pertanto inevitabile che la gamma delle competenze cui i comuni riescono a far fronte risulti molto variabile, pur considerando la differente «dimensione» – economica, gestionale o quant'altro – che la medesima attività comporta al variare delle dimensioni del comune; a ciò si aggiungono le differenze dovute alle caratteristiche, quali ad esempio la collocazione geografica o l'importanza o meno della locale componente storico-artistica, fattori che inducono necessariamente a prestare attenzione nella prassi, a determinati temi a scapito di altri.

Il secondo aspetto, anch'esso fonte di differenziazioni, è appunto la produzione legislativa ai vari livelli dell'organizzazione amministrativa: questa produce una struttura gerarchica («gerarchia delle fonti») per cui i comuni se da un lato, nell'emanare le proprie regole, devono tenere presente anche ciò che è stato legiferato a livello regionale e statale, dall'altro la loro prassi è influenzata da questi due «livelli» normativi oltre che dal loro proprio: mentre la legislazione statale non produce fattori di differenziazione o, se li produce, lo fa in termini generali, d'inquadramento, con un certa valenza strategica, quella regionale può incidere significativamente nel differenziare i compiti dei comuni da regione a regione, o per lo meno nel determinare dove le amministrazioni comunali debbano focalizzare l'attenzione, su determinati temi piuttosto che su altri; a ciò si aggiunge la produzione normativa locale che introduce differenze tra comuni della medesima regione. Questo scenario ha avuto inevitabili conseguenze negative sul fronte dell'informatizzazione dei processi che si svolgono nei comuni, quando non è stato l'alibi per lo svilupparsi di situazioni che hanno successivamente rivelato un elevato livello di criticità: l'aspetto più evidente è che oggi vi è una differenziazione molto significativa negli usi della tecnologia Ict e, conseguentemente, nei risultati che se ne ottengono.

Ad un esame più attento si osserva che, in realtà, esiste una sorta di «soglia critica», esprimibile in numero di abitanti, al di sotto della quale la diffusione delle tecnologie, pur essendo ovviamente possibile, non riesce a produrre i vantaggi che ne potrebbero derivare. Questa «soglia critica» non è rappresentata da un unico valore, valido per qualsiasi problema venga affrontato, ma è in realtà costituita da diversi valori, in funzione del particolare tema o funzione che viene coinvolta dal processo di informatizzazione: ad esempio, pur non considerando i comuni molto piccoli – per i quali occorrerebbe fare considerazioni specifiche, nella prospettiva di creare forme di aggregazione che ne facilitino e semplifichino l'approccio alla tecnologia in modo efficiente e senza spreco di risorse finanziarie – al di sotto dei 30.000 abitanti si ha efficacia nell'uso delle tecnologie Ict con soluzioni «in proprio» sostanzialmente solo per alcune funzioni di base, quali bilancio, personale, servizi demografici e qualche altro servizio con forte valenza operativa; al di sotto dei 50.000 abitanti alcune applicazioni, quali quelle dell'area territorio e catasto, particolarmente utili per la lotta all'evasione fiscale (tema di prossima competenza anche comunale) risultano in realtà assolutamente diseconomiche, anche solo per i costi che comportano le attività di *data cleaning* che sono necessarie, e quindi non in grado di fornire i vantaggi promessi o attesi. Queste osservazioni portano a evidenziare l'esistenza, appunto, di limiti di «massa critica» nelle funzioni svolte dai comuni, al di sotto dei quali l'utilizzo delle tecnologie diventa non più economicamente vantaggioso o, in altre parole, rimane ampiamente al di sotto delle potenzialità che potrebbe esprimere.

4.3.1.1. Lo stato della diffusione della tecnologia

Per meglio chiarire queste considerazioni, e a loro integrazione, è utile analizzare brevemente come si è sviluppato il processo di diffusione delle tecnologie Ict nei comuni: i primi ad essere interessati sono stati, ovviamente, quelli di maggiori dimensioni, che hanno iniziato ad introdurre le tecnologie nelle aree di maggior peso amministrativo (contabilità, bilancio, personale), seguite molto presto da quelle legate ai servizi demografici e, successivamente, da quelle di altre aree funzionali. Nel tempo il processo si è diffuso, seguendo l'evoluzione tecnologica e la relativa diminuzione dei costi dell'hardware, interessando i comuni di dimensione via via decrescen-

te: mano a mano che si rendevano disponibili sistemi di dimensioni minori, nello stesso modo si abbassava la soglia minima di introduzione della tecnologia. In questo processo la logica seguita è stata del tipo «un *computer* per ogni campanile», privilegiando quindi la presenza fisica delle infrastrutture tecnologiche piuttosto che le funzioni che queste rendevano disponibili (a questo proposito va comunque sottolineato che, nel periodo cui ci si riferisce, erano già tecnologicamente possibili soluzioni di tipo «consortile» che, raggruppando più comuni, avrebbero potuto superare i problemi di efficacia legati alle «soglie critiche» cui si è accennato in precedenza). Il risultato finale è stato una diffusione disomogenea e non coordinata di soluzioni applicative, differenti tra loro rispetto alle funzioni interessate e alle modalità di implementazione; non si sono cioè neppure fatte le considerazioni precedenti sulla «massa critica» delle funzioni informatizzate, preferendo adottare soluzioni di «ampiezza» decrescente (intesa come grado di copertura delle funzioni), secondo la dimensione dei comuni che venivano coinvolti, fornendo così soluzioni applicative sostanzialmente incomplete e parziali.

Un altro esempio è utile per comprendere meglio la situazione come oggi risulta: è noto che la gestione del territorio è posta in capo alle regioni: avviene che queste sviluppino dei sistemi informativi territoriali (Sit) estremamente completi e raffinati, che producono una amplissima gamma di dati e informazioni potenzialmente molto utili: quando però i dati vengono inviati ai comuni per le necessarie attività di verifica e validazione, capita che questi non siano in grado di effettuare tali controlli per mancanza degli appositi strumenti tecnologici e delle relative risorse umane, vanificando così gli investimenti delle regioni; ciò avviene, naturalmente, soprattutto per i comuni più piccoli che, tuttavia, non necessariamente gestiscono porzioni piccole di territorio anzi, al contrario, spesso gestiscono aree molto vaste (basti pensare ai comuni di montagna, dove peraltro la gestione del territorio è tema di grande rilevanza). Questo esempio evidenzia un *modus operandi* nel processo di diffusione della tecnologia privo di una visione integrata della realtà dei comuni e delle funzioni che sono chiamati a svolgere.

A proposito del processo di diffusione della tecnologia nei comuni (ma non solo, la tendenza è presente, con le dovute specificità, anche in altri settori) è utile sottolineare un altro fenomeno: nel corso degli anni l'offerta si è spostata da soluzioni *ad hoc* verso soluzioni a pacchetto, in modo particolare per quello che riguarda gli enti di minori dimensioni, proposta da aziende di dimensioni medie e piccole; il comparto industriale ha tuttavia iniziato a vedere un processo di aggregazione e di acquisizione di aziende con il risultato di un significativo consolidamento: purtroppo ciò non è stato seguito da un contestuale processo di «svecchiamento» tecnologico delle soluzioni offerte, con il risultato che sono ancora ampiamente diffuse soluzioni in architettura *client server*, quando non soluzioni in qualche modo integrate con applicativi di *office automation*, entrambi non erogabili in modalità *cloud*.

Volendo riassumere le caratteristiche e le criticità che la situazione dei comuni oggi presenta si può affermare che vi è disomogeneità nella diffusione delle tecnologie, polverizzazione delle soluzioni che spesso, per la dimensione del comune o per la loro «anzianità», non riescono ad essere efficaci rispetto ai compiti delle funzioni amministrative, elevata variabilità delle soluzioni con conseguente mancanza di standard nella struttura dei dati e nella loro semantica, che rendono problematica qualsiasi attività di scambio di dati: a fronte di una situazione che è quindi caratterizzata da una grave mancanza di efficacia complessiva, i comuni italiani, secondo le principali aziende di studi di mercato, spendono circa 550 milioni di euro all'anno.

4.3.1.2. Due casi critici

Ciò detto, al fine di fornire ulteriori elementi di valutazione, è utile considerare due situazioni particolari, scelte proprio per il «contrasto» tra bisogni dei comuni e capacità delle soluzioni tecnologiche di soddisfare tali bisogni: l'area catasto/tributi e l'area edilizia privata. A giustificazione della scelta, va sottolineato che, considerando la situazione economica attuale e prevedibile a breve periodo, ed il suo impatto sulle disponibilità economiche dei comuni, soluzioni di automazione di questi settori adeguatamente implementate potrebbero fornire un decisivo contributo nel recupero di risorse fi-

nanziarie oggi non disponibili. Va infine ricordato, in una prospettiva di evoluzione della situazione attuale, che le linee lungo le quali si sta definendo lo sviluppo della produzione legislativa relativa al federalismo, linee per altro auspicabili, prevede il trasferimento della capacità impositiva ai comuni e la creazione, per quelli con meno di 5.000 abitanti, di aggregazioni cui andranno delegate le funzioni proprie dei comuni, probabilmente con eccezione del bilancio; si è quindi in presenza di una considerevole opportunità che potrebbe facilitare l'introduzione di soluzioni tecnologiche avanzate, in quanto l'attività di riorganizzazione, che inevitabilmente dovrà aver luogo, potrebbe essere associata ad un intervento teso a rivedere, razionalizzare e semplificare le attività amministrative attualmente esistenti nell'area della gestione dell'edilizia privata e del catasto, attività, come detto, necessariamente preliminare a qualunque intervento sistematico di soluzioni tecnologiche nelle aree stesse.

Il caso catasto/tributi

Lo stato dell'arte dell'automazione dell'area tributi nei comuni si presenta estremamente diversificato: anche i progetti più evoluti soffrono sia per mancanza di competenze approfondite sul versante dei processi e, più specificatamente, degli aspetti tecnologici, sia per mancanza di coordinamento tra i differenti livelli dell'amministrazione pubblica centrale e locale; va inoltre sottolineato che le norme attuali richiedono la trasmissione di consistenti moli di dati al Ministero dell'economia, ma i comuni non riescono a soddisfare tali richieste per mancanza di risorse e di adeguati strumenti tecnologici: ne consegue una ridotta interazione tra strutture centrali e periferiche della pubblica amministrazione, quali l'Agenzia del territorio e l'Agenzia delle entrate con conseguente riduzione dell'efficacia dell'azione delle amministrazioni e danni al sistema sociale ed economico.

Lo sviluppo legislativo, legato al procedere del federalismo fiscale, prevede un ampliamento delle relazioni tra centro e periferia, dovuto a una diversa distribuzione dei compiti, a seguito del ridisegno della capacità impositiva degli enti e, in particolare, la necessità, da parte dei comuni, di accedere in modo più ampio ai dati fiscali oggi detenuti dal Ministero dell'economia; tralasciando le complesse questioni legislative legate al tema della salvaguardia della *privacy* e a tutti gli aspetti connessi con esso, lo sviluppo previsto comporterà necessariamente un'evoluzione dei sistemi informativi comunali (e non solo) per adeguarli alle nuove esigenze ed ai nuovi compiti; questa prospettiva tuttavia dovrà confrontarsi con gli aspetti strutturali che caratterizzano oggi i dati: va infatti ricordato, ad esempio, che i catasti comunali sono significativamente differenti per struttura dei dati e loro semantica e che manca la cartografia nazionale digitalizzata che andrebbe associata alle carte tecniche del catasto; quest'ultimo aspetto è particolarmente significativo in quanto l'impossibilità di associare cartografia con carte tecniche riduce drasticamente la fruibilità dei dati, soprattutto da parte dei comuni di minori dimensioni, non in grado di gestire autonomamente le infrastrutture tecnologiche necessarie; a ciò si aggiunge un ulteriore aspetto critico dovuto alle differenze funzionali tra le diverse soluzioni applicative adottate da comuni o altri enti sovra ordinati (ad esempio le regioni) che offrono, come servizio, la gestione del catasto a gruppi di comuni.

A fronte di questo quadro critico, va comunque evidenziata l'esistenza di alcune soluzioni che si segnalano per la loro completezza ed efficacia, quali, ad esempio, quelle del Comune di Monza e della Regione Emilia-Romagna, che potrebbero, a determinate condizioni, essere assunte come soluzioni guida.

Occorre tuttavia sottolineare ancora un aspetto e precisamente quello della bassa qualità dei dati (codici fiscali errati, indirizzi sbagliati o incompleti, eccetera), elemento cruciale per la lotta all'evasione fiscale, soprattutto quella legata al patrimonio immobiliare: si consideri che, mentre il valore dei tributi comunali è stimato complessivamente in circa 52 miliardi di euro, quello afferente la base imponibile del patrimonio immobiliare è stimabile in circa 4.000 miliardi di euro e che la tassazione e l'esazione delle imposte sul patrimonio immobiliare sono destinate a divenire, come detto, compiti dei comuni, almeno in parte: è evidente quindi l'utilità ed i vantaggi che progetti di automazione del catasto correttamente impostati, che inoltre integrino anche la cartografia nazionale digitale e le carte tecniche, potrebbero portare.

È quindi evidente l'utilità, se non la necessità, di provvedere a so-

luzioni di gestione del catasto che superino tutti i problemi precedentemente esposti e, anzi, permettano il più completo interscambio dei dati: un'ipotesi da considerare può essere quella di individuare una soluzione particolarmente avanzata (di un comune o di una regione) adeguarla a tutto il territorio nazionale, in accordo con le regioni e l'Agenzia del territorio, e renderla fruibile in modalità *cloud* a tutti i comuni; tuttavia va osservato che, anche in questo caso, precondizione per la riuscita del progetto è la presenza di un organismo nazionale, con un mandato forte, che definisca gli standard dei dati necessari ai vari livelli della struttura amministrativa, sovrintenda allo sviluppo della soluzione applicativa prescelta e ne coordini il dispiegamento sul territorio nazionale.

Il caso edilizia privata

Il settore dell'edilizia privata presenta significative differenze nei modi in cui viene gestito a seconda della collocazione geografica e della dimensione del comune; il settore è soggetto ai tre livelli legislativi e regolamentari, cui si è già accennato in generale per i comuni, e precisamente quello nazionale, quello regionale e quello comunale: da ciò nascono, nei procedimenti e nella gestione dei processi amministrativi, diversità tra comuni di regioni diverse e tra comuni della stessa regione; di particolare impatto è l'intervento regolamentare a livello comunale: al di la della necessità di adattare, alla specifica realtà locale, i livelli regolamentari superiori, frequentemente vi è una sorta di esasperazione nell'interpretazione delle leggi nazionali e regionali e nella loro articolazione, ad esempio, in sede di stesura del regolamento edilizio che crea, a volte anche artificialmente, particolari complessità e ostacoli nello svolgimento dei processi burocratici; uno degli aspetti più delicati che ne consegue è che il personale comunale addetto all'edilizia privata ha competenze molto specifiche e specializzate, «verticalizzate» sui provvedimenti di ogni singolo comune, e risulta quindi molto difficile da «disintermediare» come potrebbe avvenire con opportune soluzioni tecnologiche standard: a questo proposito va detto che i principali ostacoli, a progetti di automazione delle attività legate all'edilizia privata, sono venuti proprio dal personale comunale che dovrebbe utilizzarle, in quanto vi vede il pericolo di una propria marginalizzazione (o disintermediazione) e, va purtroppo detto, di un aumento della trasparenza delle procedure, con conseguente riduzione dell'area della propria discrezionalità.

Risultato di tutto ciò è che il settore dell'edilizia privata è molto scarsamente informatizzato e, nei pochi casi ove la tecnologia è presente, questa risulta prevalentemente utilizzata per «tracciare» i soli procedimenti autorizzativi, con la gestione di una quantità di dati estremamente limitata e di livello non rilevante: non si tratta infatti di applicazioni che gestiscono l'intero processo autorizzativo, ma bensì che riguardano solo sue parti, quasi «appunti» relativi al processo, tant'è vero che nessun comune dispone di un archivio strutturato dei procedimenti avvenuti. Conseguentemente non esiste una banca dati digitale che costituisca il «consolidato» dei risultati delle attività dei comuni nell'area dell'edilizia privata, cioè sugli immobili: unico esperimento è quello promosso da comuni, Anci, regioni e Agenzia del territorio e noto come «Anagrafe comunale degli immobili» che mira a realizzare una anagrafe immobiliare unitaria, attraverso l'integrazione dei dati di origine comunale con quelli catastali e il data base topografico regionale. Ma si tratta appunto di un esperimento.

Preliminari a un intervento su larga scala nel settore dell'edilizia privata sono comunque alcune azioni:

– rivedere la produzione legislativa nell'ottica di rimuovere alcuni vincoli normativi, razionalizzare e semplificare gli aspetti procedurali, oggi complessi e frequentemente poco chiari e che finiscono con il permettere, a volte, una gestione non completamente trasparente delle procedure;

– definire un modello digitale unico per l'edilizia, definendo in modo univoco le informazioni rilevanti a livello nazionale, quindi un set di dati standard a partire dai quali sia comunque possibile integrare gli archivi per attività basate su piani regolamentari diversi per i vari livelli amministrativi, secondo le specifiche esigenze e caratteristiche del territorio di competenza.

Un simile intervento dovrebbe mirare a:

– sul versante del *front end*, semplificare la redazione delle pratiche edilizie per cittadini e professionisti, permettendo loro anche di verificare lo stato di avanzamento delle pratiche, tramite l'accesso

agli opportuni archivi comunali;

– sul versante del *back end*, mettere a disposizione dei funzionari comunali uno strumento per la gestione delle pratiche che garantisca migliore qualità e minore attività di istruttoria.

Nel processo descritto le regioni dovrebbero avere un ruolo chiave, date le loro competenze in materia di gestione del territorio e la loro capacità normativa, per imporre ai comuni l'implementazione delle scelte e delle direttive, da loro stesse predisposte.

Allo Stato, o meglio a una struttura nazionale con un mandato forte, deve restare il ruolo di governo dei processi ed in particolare di promozione e implementazione dei primi due punti precedentemente indicati. Un intervento come quello descritto è inoltre urgente anche per la presenza, in materia di edilizia privata, di una serie di soggetti (enti pubblici, aziende, ordini professionali) che a vario titolo se ne occupano, e il cui attivismo in materia d'informatizzazione delle procedure non sempre risponde a obiettivi e interessi generali.

4.4. Il modello proposto

È innegabile che le tecniche di *cloud computing* permettano oggi di porre rimedio alle criticità precedentemente indicate, permettendo che ogni comune disponga, all'occorrenza, non solo di tutte le soluzioni di cui necessita ma anche nella loro massima ampiezza funzionale: occorre comunque preliminarmente fare alcune osservazioni.

Nella discussione precedente si sono più volte citati i termini «funzioni» o «attività» riferendoli all'operare dei comuni: scomponendo nei suoi fattori elementari l'insieme dei loro compiti, in precedenza denominate «aree servizi», si arriva a circa 200 differenti «funzioni elementari», intese come specifiche aree di attività, distinte l'una dall'altra, ove non necessariamente ciascuna genera un risultato «finale», dato che questo può essere raggiunto anche dallo svolgimento di più «funzioni elementari» tra loro correlate; un aspetto da sottolineare è che in questa modalità operativa le singole «funzioni elementari» svolgono la loro attività in modo parallelo,

generalmente ricongiungendosi in un risultato unico, se del caso, solo alla fine. È logicamente possibile associare a ciascuna «funzione elementare» una soluzione informatica (un'applicazione) che ne automatizza i «contenuti» e il «percorso» e che in pratica ne supporta lo svolgersi; si può quindi ritenere che un comune necessiti di circa 200 «applicazioni elementari» per soddisfare tutte le proprie esigenze funzionali. Questo aspetto è molto importante per il prosieguo dell'analisi, in quanto permetterà di costruire un'ipotesi alternativa alle attuali modalità di utilizzo delle tecnologie, basata su un approccio applicativo per processi e non più per funzioni e sull'erogazione dei servizi applicativi in modalità *cloud computing*.

Abitualmente i comuni, o meglio gli amministratori e i funzionari comunali, nello svolgimento delle attività proprie del comune tendono, «inconsciamente», a utilizzare il modello basato sulle funzioni, in modo indipendente dagli obiettivi strategici dell'ente, senza cioè una visione unificante e integrata delle attività; sul piano dei processi di informatizzazione ciò si traduce ad esempio, come nel già citato caso «relazione stato/luogo» o «cittadini-territorio», nella mancata integrazione tra gli elementi degli archivi che, oltre a comportare duplicazioni dei dati e conseguenti errori, comporta spreco di risorse finanziarie e una complessiva minore capacità ed efficacia degli strumenti tecnologici a fornire soluzioni a problemi complessi e, a volte, di vitale importanza per i comuni stessi (si consideri quanto detto a proposito della lotta all'evasione fiscale).

Stante il fatto che l'archivio della popolazione e l'archivio del territorio sono i due archivi cardine dell'attività dei comuni, la prima necessità è pertanto quella di definire, a livello nazionale, una struttura standard della descrizione dei dati di questi due archivi e del sistema di relazioni che coinvolgono i singoli elementi che li compongono: questa struttura costituisce così una sorta di «architrave» del sistema informativo comunale. Per quanto riguarda gli aspetti applicativi si possono raggruppare le attività del comune in 10 macroaree, che costituiscono le «colonne» (motori di *workflow* tematici o soluzioni applicative verticali), che insistono sui due archivi precedenti, utilizzano il sistema di relazioni definito tra i due archivi e sono sviluppati integrando tutte le «funzioni elementari» di una determinata area di attività del comune, in un'ottica di gestione in-

tegrata per processi e non più per funzioni. Le 10 soluzioni applicative verticali, che possono esaurire tutte le 200 «funzioni elementari» svolte dai comuni, possono essere le seguenti, che in buona sostanza riaggregano le «aree funzionali» individuate nel modello di cui al paragrafo 4.1:

– anagrafe e stato civile
– servizi sociali
– educazione e cultura
– gestione del territorio
– area tecnica e gestione edilizia
– fiscalità e tributi
– contabilità e bilancio
– protocollo e gestione dei flussi informativi
– servizi al cittadino (*front office*)
– servizi di supporto

Lo schema presentato non costituisce un «esercizio» puramente teorico e astratto, bensì è derivato da alcune esperienze concrete, che sono in corso in alcune regioni ed enti pubblici italiani: da un punto di vista implementativo, volendolo generalizzare all'insieme dei comuni, occorrerebbe individuare le migliori soluzioni, renderle compatibili con un disegno generale simile a quello descritto sopra, quindi stabili e standard, e successivamente metterle a disposizione dei comuni.

Soluzioni come quelle delineate possono assolutamente essere rese disponibili in modalità *cloud computing*: si tratta ora di discutere quali soggetti potrebbero erogare il servizio e la numerosità dei «punti» di erogazione necessari. I due temi sono strettamente correlati: per quanto riguarda i soggetti, va osservato che, proprio per le questioni di «massa critica» accennate sopra, si può indicativamente ritenere che per i comuni con oltre 250.000 abitanti sia giustificata una soluzione in proprio, in considerazione anche delle specificità strutturali e organizzative dovute alla dimensione degli enti in questione, con la possibilità eventuale di aggregare comuni limitrofi di minori dimensioni. Negli altri casi si può pensare a meccanismi, anche di tipo finanziario, che comunque potrebbero essere utilizzati anche nel caso precedente, rivolti a favorire la creazione di aggregazioni di comuni che deleghino la gestione informatizzata delle proprie funzioni alla struttura di aggregazione: si può cioè ipotizzare un sistema di incentivi finanziari per quei comuni che si aggregano, ad esempio attorno ad un comune maggiore, e che utilizzano soluzioni Ict da esso fornite come servizi in modalità *cloud*. Gli erogatori del servizio possono quindi essere i comuni stessi, ma nulla è di ostacolo a che vi possano essere anche entità private o, ad esempio, aziende di scopo pubblico-private, tutte opportunamente certificate, che eroghino a loro volta i servizi di cui necessitano i comuni. L'elemento decisivo rimane l'utilizzo del medesimo progetto applicativo in tutto il territorio nazionale. Per quanto riguarda la numerosità dei «punti» di erogazione dei servizi, escludendo i 12 comuni con oltre 250.000 abitanti, dotati ciascuno di una propria soluzione, si può ipotizzare un numero di tali «punti», funzione della numerosità dei comuni e della popolazione residente nelle regioni, indicativamente variabile da 12 a 20; l'ampia variabilità indicata è dovuta al fatto che il presente documento non costituisce uno studio di fattibilità del progetto, con quindi tutte le indicazioni a carattere implementativo del caso, ma una descrizione realistica di un possibile modo, alternativo ed implementabile, di informatizzazione delle attività dei comuni, che superi gli inconvenienti indicati in precedenza, che si riscontrano nella situazione odierna e che limitano fortemente l'efficacia delle soluzioni tecnologiche sino ad ora adottate. D'altra parte il numero dei «punti» di erogazione del servizio non incide in modo particolarmente significativo sui costi, some si vedrà nel seguito.

Al fine di una completa descrizione del progetto resta da discutere chi possano essere gli enti cui delegare lo sviluppo del progetto applicativo e quale possa essere la struttura di *governance*: i due temi sono, anche in questo caso, correlati. Con riferimento al primo tema, si è detto che il progetto ipotizzato trae spunto da esperienze in corso presso alcuni enti pubblici italiani e si è detto della possibilità di individuare le migliori soluzioni e renderle disponibili in un contesto integrato come quello descritto; vi è poi l'aspetto della distribuzione delle soluzioni sul territorio nazionale e l'attività di certificazione delle strutture eroganti il servizio; i temi hanno forti relazioni tra loro e pongono inequivocabilmente il problema della crea-

zione di una struttura nazionale in grado di gestire tutti gli aspetti che concorrono alla definizione e all'implementazione del progetto. La struttura, in collaborazione con le regioni, dovrebbe: definire le linee strategiche ed operative del progetto, definire gli standard in termini di dati e di applicazioni, individuare le soluzioni migliori, coordinarne lo sviluppo e l'integrazione, individuare i «centri» di erogazione, effettuare le attività di certificazione delle strutture eroganti il servizio, sovraintendere al dispiegamento delle soluzioni, gestire gli aspetti finanziari del progetto ed in particolare gli incentivi ai comuni che si volessero aggregare. Si deve trattare quindi di una struttura con un mandato forte cui venga delegata, come detto, l'implementazione del progetto in tutti i suoi aspetti.

Non si può negare che una soluzione come quella descritta comporta significativi impatti anche sul piano dell'organizzazione delle attività dei comuni, e forse più in generale degli enti pubblici; ma più che la soluzione è l'approccio per processi ad avere impatti: questo infatti comporta interventi, sul piano dell'organizzazione e del *modus operandi* degli enti, che forniscano una visione e una concezione integrata dell'operare degli enti stessi, altrimenti non sarà possibile superare l'attuale situazione di stallo. Un'ipotesi potrebbe essere che la struttura nazionale, cui si è accennato sopra, svolga un'opera di sensibilizzazione su questi temi e di «suggerimento» al legislatore di eventuali interventi suoi propri nella prospettive di evolvere le modalità operative verso quella direzione.

4.4.1. I costi

Per la determinazione dei costi si sono considerati separatamente il costo di implementazione dell'archivio integrato «cittadino-territorio» (cioè dell'archivio costituito dai dati descrittivi dei singoli elementi e dalle relazioni che intercorrono tra loro) e dei singolo motori di *workflow* (soluzioni applicative verticali); tali costi, rilevati presso enti che stanno muovendosi in queste direzioni, sono risultati pari a 5 milioni di euro per gli archivi e, mediamente, pari a 1 milione di euro per ogni motore di *workflow*; la stima complessiva di costo per la realizzazione *ex novo* di un progetto come quello descritto è quindi pari a circa 15 milioni di euro.

A fronte dei costi per lo sviluppo, quindi da sostenersi una sola volta, vi sono i costi di gestione della piattaforma applicativa; tra questi vi sono i costi di aggiornamento e manutenzione della soluzione e i costi propriamente di gestione: i primi sono stimabili in circa 1, 2 milioni di euro e vengono spesi «una volta sola», in quanto l'applicazione è comune a tutti.

Per quanto riguarda i secondi, cioè i costi annuali sostenuti per l'utilizzo delle applicazioni, questi possono essere stimati in base alle seguenti ipotesi: per i 12 comuni con oltre 250.000 abitanti e per i 16 «punti» di erogazione del servizio (assumendo un valore medio tra i due di massima e minima indicati in precedenza), che utilizzano quindi ciascuno una «copia» della soluzione, si mantengono sostanzialmente uguali i costi per l'hardware, si riducono i costi per software di base e *tools* (sostituiti da servizi IaaS e PaaS), si annullano quelli per software applicativo e si riducono i costi per servizi, in particolare si annullano quelli per servizi di supporto allo sviluppo, mentre rimangono, in una percentuale stimabile pari al 15%, come attività consulenziale di supporto alle fasi di sostituzione (*change*) e di successiva gestione del progetto.

Per tutti gli altri comuni si annullano i costi per *server* e relativi software di sistema e applicativi ed i costi per servizi tranne una componente, stimabile come sopra pari al 15%, per attività di supporto al processo di sostituzione e successivamente di gestione del progetto.

Lo scenario che si viene a delineare non è sostanzialmente dissimile da quanto descritto nel caso del fascicolo sanitario elettronico; come in quel caso ulteriori riduzioni di costo si possono individuare in una molteplicità di situazioni, che qui si elencano sinteticamente, rimandando al caso già discusso del Fse per una loro descrizione più dettagliata (fatto salvo le ovvie differenze derivanti dalle rispettive aree di attività degli enti coinvolti):

– riduzione delle dotazioni hardware e relative spese di gestione e manutenzione;

– riduzione spese di manutenzione adeguativa e correttiva del software applicativo;

– riduzione della spesa di adeguamento tecnologico;

– riduzione della spesa per le componenti software di sistema;

– riduzione delle spesa a seguito all'adozione di standard dei dati.

La spesa per integrazione di applicativi non viene considerata, in quanto non presente nelle voci di spesa odierna, per la mancanza stessa del tipo di attività. Per il calcolo dei costi si sono applicati criteri simili a quelli utilizzati per il Fse e il medesimo metodo: si sono rilevati i costi attualmente sostenuti da comuni di differenti dimensione per le diverse voci di spesa, e si sono riproporzionati secondo le componenti di spesa It i cui valori, a livello dell'intero comparto della pubblica amministrazione locale, sono maggiormente diffusi.

– si è assunta come spesa It complessiva dei comuni il valore indicato dalle principali società di analisi di mercato pari a 550 milioni di euro;

– sulla base dei dati raccolti presso comuni di varie dimensioni si è stimata una spesa annua di circa 180 milioni di euro per hardware, circa 70 per software e circa 300 per servizi, di gestione e di sviluppo;

– si sono quindi effettuate le stime della spesa attuale per i 28 «punti» di diffusione delle soluzioni in *cloud* come indicato in precedenza (12 città con oltre 250.000 abitanti e altri 16 «punti»), assumendo che questi possano esser considerati come i «maggiori» spenditori: sulla base della media dei dati raccolti relativi alla spesa dei comuni «maggiori», la stima della spesa attuale relativa ai 28 «punti» è pari a 172 milioni di euro l'anno, di cui 56 per hardware, 22 per software e 94 per servizi;

– si sono applicate alle singole voci di spesa rilevate presso i comuni «maggiori», cioè i 28 «punti» di erogazione delle soluzioni in *cloud*, le *variazioni* come indicato in precedenza ottenendo la spesa al netto degli effetti dell'applicazioni di soluzioni *cloud computing*; tale spesa, per i 28 comuni, è risultata pari a 70 milioni di euro l'anno;

– per i rimanenti comuni, cui oggi si può attribuire una spesa complessiva pari a circa 380 milioni di euro, con una evidente ampia variabilità nei valori della spesa media data la variabilità dimensionale dei comuni stessi, applicando i medesimi criteri di cui sopra, si perviene ad una stima complessiva pari a circa 130 milioni di euro l'anno.

In sintesi a fronte di una spesa annua attuale prossima a 550 milioni di euro, la soluzione delineata sopra ed erogata in modalità *cloud computing* avrebbe un costo di realizzazione pari a circa 15 milioni di euro ed un costo di esercizio pari a circa 200 milioni di euro l'anno, oltre a tutti gli evidenti vantaggi funzionali cui si è fatto cenno in precedenza.

A proposito della soluzione indicata, per i comuni vanno fatte le medesime osservazioni conclusive svolte per il fascicolo sanitario: non si riportano in modo analitico in quanto già discusse in quel caso: si richiamano tuttavia sinteticamente alcuni aspetti:

– necessità di una «guida» unica a livello nazionale con un mandato forte volto alla realizzazione del progetto;

– possibilità, anzi opportunità, di riutilizzo del personale che si rendesse disponibile, con compiti di supporto al dispiegamento del progetto ed alla sua successiva gestione;

– capacità innovativa del progetto e conseguente necessità di adeguati strumenti organizzativi per la sua implementazione, in particolare un sistema di *governance* «a più livelli» che dispieghi la propria azione con il supporto delle regioni, dei tecnici e degli specialisti resi disponibili presso i vari sistemi informativi dei comuni.

Un'ultima nota: si è detto sopra che il numero di «punti» di erogazione del servizio non incide in modo particolarmente significativo sui costi della soluzione *cloud*: infatti rispetto alla stima indicata sopra di 70 milioni di euro l'anno come spesa di 28 comuni erogatori della soluzione in *cloud*, tale spesa varia da 60 a 80 milioni di euro l'anno se si assumessero 24 piuttosto che 32 «punti» di distribuzione, differenza quindi non tale da alterare il quadro descritto.

5. Schema delle relazioni e flussi di processo

Il Comune è un'entità complessa con una rete di relazioni molto articolata, come si è delineato negli schemi precedenti: di fatto esso si pone al centro di un ecosistema che concretizza e agisce un numero elevatissimo di processi e di flussi informativi.

Ai fini dello studio è tuttavia utile concentrarsi solo su alcuni di essi, prevalentemente focalizzati sulle attività interne del comune e

sui suoi ruoli istituzionali, con lo scopo di identificare dei campioni rappresentativi di servizi, utili a definire delle ipotesi architetturali e tecnologiche per la definizione di servizi *cloud* atti a supportarne l'erogazione. In quest'ottica si ritiene d'interesse restringere il campo a tre processi, direttamente riferiti a servizi istituzionali erogati dai comuni, due dei quali interamente presidiati da strutture interne al comune, il terzo dipendente da una forte interazione da enti esterni.

I processi e i flussi rappresentati di seguito costituiscono comunque un primo esercizio indicativo, che può essere oggetto di ulteriore affinamento o integrazione: si reputa comunque utile svilupparli per avviare il confronto di merito anche sui possibili modelli architetturali a supporto. La descrizione dei processi espressa negli schemi che seguono è sintetica e non ha la pretesa dell'esattezza assoluta: i processi in questione vengono considerati solo nella loro valenza di esempi «astratti» di fenomeni reali; da questo punto di vista è ininfluente la loro effettiva rispondenza puntuale o meno ai processi reali, prevalendo la loro funzione di schemi logici che fanno riferimento a fatti reali; il loro scopo è esclusivamente funzionale ad esplicitare come la metodologia di analisi per processi sia concretamente applicabile a servizi, effettivamente erogati dagli enti della pubblica amministrazione. Essi vengono rappresentati, inoltre, in condizione «ottimale», senza rappresentare cioè tutte le complessità operative o quegli elementi di «attrito burocratico» che possono presentarsi nella loro declinazione operativa nelle diverse realtà locali: si presentano pertanto come una sorta di «processo ideale», pur considerando tutti i passaggi attualmente previsti dalla normativa e dalla prassi operativa corrente. Infine, non si indicheranno eventuali strumenti di automazione possibili sulla base di soluzioni «tradizionali», riservando l'analisi di eventuali soluzioni di automazione a supporto ad una fase successiva di definizione delle possibili architetture in *cloud*.

Il primo flusso è riferito al processo di dettaglio che si colloca nell'ambito dell'edilizia privata e riguarda il servizio di gestione della domanda di nuove concessioni edilizie (permesso di costruzione) Il diagramma di flusso della figura che segue rappresenta le attività del processo e gli attori coinvolti: il flusso di attività è mono-direzionale e veicola esclusivamente documenti; non esistono tempi di attraversamento definiti o vincolanti se non quelli definiti dalla procedura civile per eventuali contenziosi.

In sintesi:

– cittadini, imprese o studi professionali presentano una domanda di nuova concessione edilizia;

– la struttura deputata del comune effettua le valutazioni richieste per legge e:

  – rilascia la concessione edilizia;

  – rifiuta la concessione, rinviandola al richiedente;

– nel primo caso, si procede all'esecuzione dei lavori;

– la struttura del comune procederà poi ai controlli di merito e potrà:

  – concedere l'abitabilità ed effettuare le opportune segnalazioni al catasto;

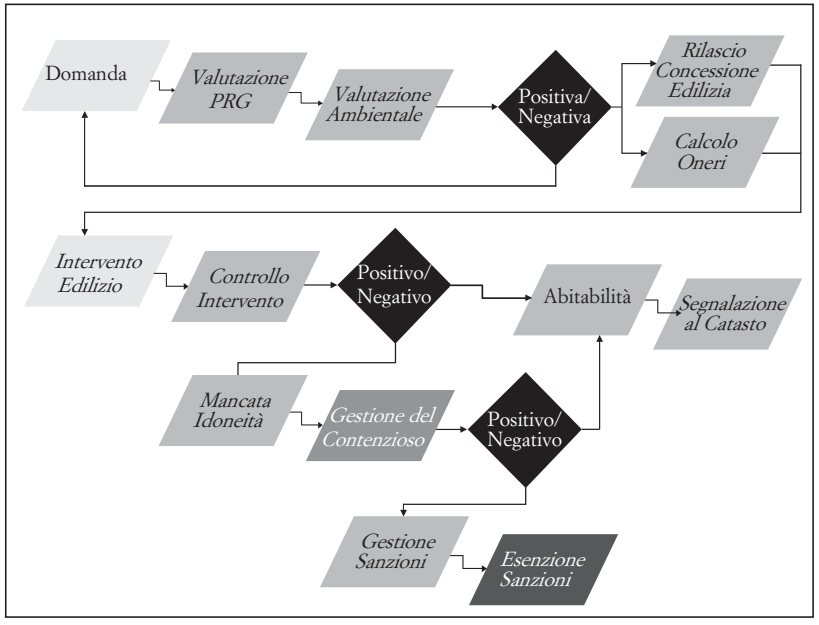
  – negare l'abitabilità, avviandosi ad una potenziale gestione del contenzioso, coinvolgendo l'avvocatura comunale;

– in questo caso, a fronte dell'esito del contenzioso, si potrà:

  – concedere l'abitabilità ed effettuare le opportune segnalazioni al catasto

  – negare definitivamente l'abitabilità, procedendo anche alla fase sanzionatoria.

Figura 11. Il processo di gestione della domanda di concessioni edilizie



In questi termini il processo si qualifica come un flusso unico con alcuni snodi decisionali in carico ad interlocutori precisi e momenti di innesto e di arresto precisamente definiti.

Il secondo flusso è riferito a un processo, sempre in ambito edilizia privata, ma riguardante la gestione dell'abusivismo.

Il processo ha caratteristiche di maggiore semplicità rispetto a quello precedente.

L'innesto è rappresentato da una segnalazione di abuso edilizio.

– viene presentata una denuncia o viene effettuato un sopralluogo a fronte del quale viene riscontrato l'abuso;

– questo viene valutato secondo i requisiti normativi e regolamentari;

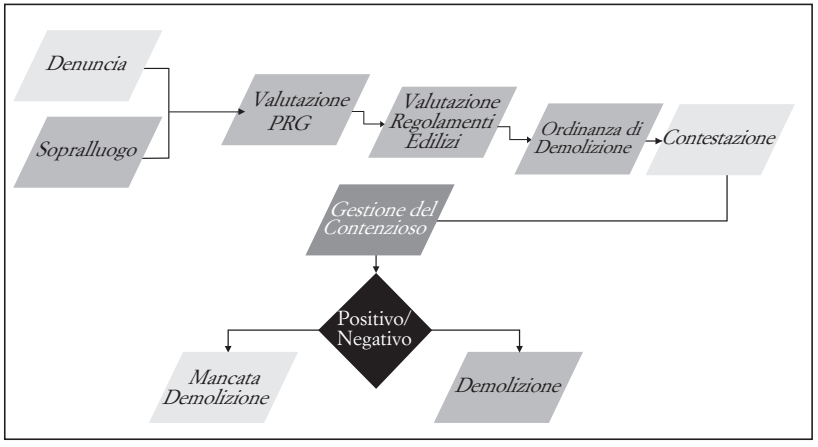
– in seguito alla valutazione viene emessa un'ordinanza di demolizione a fronte della quale può avvenire una contestazione;

– si avvia quindi la gestione del contenzioso, a fronte del quale si potrà:

– avviare la demolizione;

– sanare l'abuso mantenendo attivo l'immobile.

Figura 12. Il processo di gestione dei fenomeni di abusivismo edilizio



Anche in questo caso il processo si qualifica come un flusso unico con alcuni snodi decisionali in carico ad interlocutori precisi e momenti di innesto e di arresto precisamente definiti.

L'ultimo flusso più che un singolo processo definisce i flussi informativi e di comunicazione a supporto di diversi processi che comportano l'attivazione di un canale di finanziamento e pagamento.

In sintesi:

– il comune riceve dei fondi:

– da enti esterni;

– per esazione diretta di tributi o sanzioni;

– con tali fondi la tesoreria gestisce le procedure operative di pagamento di salari o di beni e servizi.

In questo caso gli elementi di interesse sono legati a diversi elementi:

– i flussi non sono documentali ma finanziari e dipendenti da canali differenti:

– quello interbancario standard (la tesoreria operativamente agisce attraverso canali bancari sia in ingresso che in uscita), rispetto al quale il servizio deve conformarsi alle esigenze di comunicazione proprie del canale interbancario, regolato da standard esterni alla Pa e gestito da enti regolatori sempre esterni alla Pa (es. Banca d'Italia);

– quello diretto dell'esazione di tributi e sanzioni che possono o essere direttamente veicolati tramite i canali interbancari o indirettamente tramite versamenti fisici in valuta all'esattoria, che poi effettua i trasferimenti tramite canali bancari;

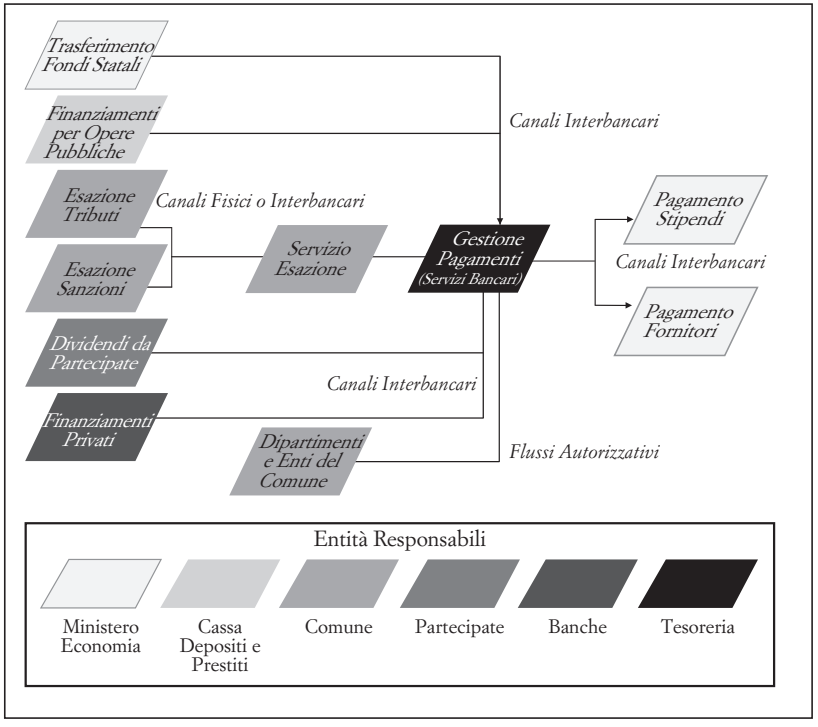
– esiste comunque una serie di flussi, non finanziari ma documentali, riferiti all'interazione tra i diversi enti e dipartimenti del comune e la Tesoreria, anche a fini autorizzativi per i pagamenti, che di fatto si avvalgono pesantemente anche dei servizi di comunicazione di base legati al protocollo, come descritto funzionalmente sopra (paragrafo 4.2);

– gli attori sono eterogenei e spesso esterni non solo al perimetro del comune ma anche a quello della Pa, pur agendo talvolta per suo conto;

– il servizio rappresenta una componente abilitante per l'erogazione di altri servizi e per l'agibilità di gran parte dei processi, rappresentando di fatto il canale di alimentazione finanziaria per la gestione operativa della struttura;

– i percorsi decisionali sono indipendenti dalla gestione dei flussi che invece richiedono solo dei momenti autorizzativi, spesso riferiti più alle specifiche del circuito interbancario che a quelli specifici dei processi supportati (es. autorizzazione di pagamento per l'emissione di un bonifico).

Figura 13. Il processo di gestione economico-finanziaria



Su questa base, i modelli di automazione di questi flussi dovranno focalizzarsi soprattutto sulla parte non finanziaria, essendo questa di fatto già gestita dagli standard bancari, prevedendo però la capacità di interagire in qualche modo con essi per la gestione dei flussi previsionali e autorizzativi.

CAPITOLO TERZO

LA *GOVERNANCE*

1. Premessa

Per comprendere i reali benefici del *cloud*, ai fini della progressiva interconnessione digitale degli enti della pubblica amministrazione italiana, può essere utile cercare di superare la dimensione strettamente «verticale» della singola organizzazione, per analizzare la natura fortemente pervasiva di questo nuovo modello di *service procurement*, in grado di diventare, potenzialmente, la piattaforma abilitante di un nuovo modello di creazione di valore pubblico nel nostro paese.

A differenza del mondo privato, nel quale la natura «indipendente» delle varie aree di attività (produttiva, distributiva o di servizio) e valutazioni strategiche di posizionamento potrebbero suggerire scelte individuali nell'adozione di strategie di *cloud computing*, per il settore pubblico, caratterizzato in modo «nativo» da una logica di «interconnessione» funzionale tra gli enti, già a prescindere dall'utilizzo delle tecnologie, nel momento del loro utilizzo prevale l'esigenza di un approccio che permetta di sviluppare, attraverso una visione organica e trasversale, una migliore comprensione dei fenomeni e delle loro possibili interdipendenze; si impone cioè un approccio di tipo sistemico, quale quello necessario nel caso di adozione di soluzioni in *cloud computing*: si è in realtà di fronte ad una situazione caratterizzata da una relazione «biunivoca», nel senso che se le caratteristiche della pubblica amministrazione impongono un approccio sistemico, d'altra parte la stessa logica delle soluzioni in *cloud* impongono un medesimo approccio.

La cosa che appare più evidente è che le forze che stanno oggi rimodellando la geografia infrastrutturale della pubblica amministrazione italiana sembrano svilupparsi lungo direzioni apparentemente contrastanti: mentre, infatti, il principio di sussidiarietà (e la stessa spinta verso uno Stato federale) tendono ad agire dal centro alla periferia, in modo che le attività possano essere svolte dall'entità amministrativa più vicina ai cittadini, dall'altra le logiche che governa-

no l'organizzazione e la distribuzione delle tecnologie (determinate anche dalla spinta alla riduzione dei costi e alla razionalizzazione delle infrastrutture) suggeriscono di muoversi in direzione contraria, e questo per l'evidente necessità di ricercare economie di scala e forme innovative di coordinamento e condivisione di risorse; il problema è che non esiste un livello ottimale nel quale concentrare la gestione delle tecnologie e delle relative competenze che sia comune a tutti i servizi: per alcuni tale punto potrebbe corrispondere con un determinato livello dello stato federale, per altri potrebbe coincidere con un livello diverso, più adeguato perché magari più adatto a garantire una più soddisfacente economia di scala o anche una garanzia di minore discriminazione su base territoriale per i cittadini.

In questo scenario il *cloud computing* potrebbe consentire una distribuzione delle tecnologie non statica e predeterminata, ma funzionale alla migliore erogazione dei servizi, favorendo, in ultima analisi la nascita di poli di erogazione specializzati per i diversi servizi. Affinché ciò avvenga, occorre prevedere la realizzazione di una serie di servizi minimi di coordinamento e di gestione, che facilitino la realizzazione di quelle condizioni, abilitanti a livello di ecosistema, capaci di assicurare le adeguate interconnessioni funzionali e di valore lungo l'intera filiera pubblica, ciò anche in considerazione del fatto che il problema non è solo la *governance* interna della singola organizzazione, ma del sistema nel suo complesso.

1.1 Lo schema di riferimento

Nel seguito si delineeranno alcuni dei fondamentali elementi di *governance* dell'ecosistema pubblico che dovrebbero svilupparsi su tre piani concettualmente distinti:

1. il primo è quello legato alla necessità di creare, come più volte richiamato in questo documento, una visione organica e trasversale dei fenomeni attraverso la definizione di opportuni sistemi di coordinamento e di orchestrazione. Tra gli elementi più importanti, a questo livello, si ricordano:

    a. un'*architettura di riferimento* per il *cloud computing* nella pubblica amministrazione che definisca i componenti funzionali e gli standard necessari per lo sviluppo e l'erogazione di servizi It in modalità *cloud*. L'adozione di un *framework* nell'ambito della pubblica amministrazione permette di realizzare componenti e funzionalità integrabili, nell'ambito di una soluzione complessiva, attraverso l'aderenza agli standard. In tal modo singoli componenti, anche se collocati in differenti amministrazioni o sviluppati da fornitori diversi, potranno integrarsi e costituire una infrastruttura unitaria che rappresenterà a tendere il *cloud* dell'intera pubblica amministrazione. Il *framework* permette di indirizzare e condividere gli standard e le modalità di implementazione della piattaforma di erogazione e dei servizi i quali, per essere erogati in modalità *cloud*, devono essere progettati con caratteristiche specifiche. Con «architettura di riferimento» s'intende quindi indicare non solo l'insieme di requisiti, componenti funzionali e politiche di gestione da adottare in base al ruolo che si intende assumere nel modello *cloud* (come indicato nel paragrafo «Impatto sull'organizzazione aziendale»), ma un vero e proprio processo di ecosistema, che punti a definire una visione architetturale condivisa e ne gestisca l'intero ciclo di vita (definizione, pubblicazione, aggiornamento, ecc.); un tale processo dovrà essere ovviamente gestito da uno o più soggetti capaci di operare una sintesi tra le esigenze che devono essere portate a livello di modello e quelle che possono restare ad un livello di caso più specifico;

    b. un *modello decisionale*, basato su parametri e metriche oggettive, che consenta alle amministrazioni di adottare decisioni coerenti al modello condiviso e, quindi, congruenti ad una visione di maggiore efficienza strutturale del sistema. Il modello decisionale dovrebbe prevedere anche servizi «consulenziali» di valutazione del rischio per l'adozione del modello *cloud*, di contrattualistica rispetto ai servizi da acquisire/da vendere e di competenza specifica su temi come gli standard d'interoperabilità e di integrazione dati. Tale modello decisionale dovrebbe anche fornire informazioni utili per consentire, ai decisori pubblici, di effettuare scelte finalizzate alla aggregazione delle infrastrutture e/o alla condivisone delle diverse strategie di servizio a livello di filiera e/o di ambito ter-

ritoriale;
c. un *sistema di pubblicazione e certificazione* che agisca da «sistema informativo» di supporto al processo di evoluzione del *cloud* nella pubblica amministrazione, e che permetta di condividere, in maniera sicura e certificata, informazioni, processi, piani di investimento e intenzioni di infrastrutturazione dei diversi attori, al fine di facilitare la nascita di aggregazioni e iniziative condivise e sinergiche.

2. Il secondo piano da sviluppare per realizzare un sistema di *governance* è quello della *utilità condivisa*, e cioè la necessità di elaborare un approccio olistico capace di tenere in considerazione tutti gli elementi di un determinato ecosistema favorendo la condivisione di obiettivi, prassi operative e risorse. Gli elementi essenziali di un sistema di utilità condivisa dovrebbero comprendere:

a. un *sistema di gestione della conoscenza* che faciliti lo sviluppo di iniziative congiunte tra le strutture della pubblica amministrazione attraverso la messa a disposizione di strumenti di gestione delle migliori pratiche, di come favorire processi di utilità condivisa nei diversi comparti, di lezioni apprese sui diversi modelli e progetti;
b. *strumenti gestionali* quali, ad esempio, il calcolo e la valutazione dei benefici derivanti dall'aggregazione, il calcolo del dividendo dell'efficienza, il *charge back* dei servizi e, più in generale, tutti quei servizi che hanno requisiti comuni a livello di sistema della pubblica amministrazione, quali sicurezza, protezione dei dati e conformità alle norme. A questo proposito alcuni temi appaiono particolarmente importanti in un sistema complesso come la pubblica amministrazione: le diverse iniziative di *cloud service procurement* dovrebbero infatti essere basate su meccanismi trasparenti e certificati di *accounting* (per il monitoraggio dell'utilizzo delle infrastrutture e delle risorse associate) e di *charge back* (basati su metriche di costo standardizzate e condivise);
c. *criteri di migrazione* verso strutture e modelli condivisi, necessari per favorire il trasferimento di servizi, componenti e infrastrutture dai primi *cloud* realizzati verso un livello di aggregazione superiore e ottenere, così, maggiori efficienze ed economie di scala. In questo modo, attraverso un processo sinergico di aggregazione, verrà a costituirsi un luogo virtuale (una «nuvola») per la progressiva condivisione di risorse, infrastrutture e servizi a beneficio dell'intero ecosistema pubblico.

3. Il terzo piano di *governance* sistemica riguarda la *realizzazione e la gestione di sistemi ibridi*. La realizzazione della «nuvola», infatti, se da una parte permette di rendere semplice e immediato l'accesso ai servizi, mascherando la complessità dei sistemi, dall'altra richiede una maggiore capacità dell'ecosistema di gestire ambienti ibridi ed eterogenei. Per questo motivo appare particolarmente importante puntare alla definizione e gestione di una serie di componenti di *governance* sistemica volte:

a. allo *sviluppo dei portafogli applicativi* attraverso soluzioni condivise di rinnovo del portafoglio applicativo, sistemi per gestione dei listini di servizi e delle componenti, *test factory* centralizzate, ecc.;
b. alla *gestione condivisa dei servizi e dei procedimenti*, attraverso sistemi per la composizione degli Sla e forme condivise di controllo dei processi in logica *end-to-end*;
c. all'*integrazione tra ambienti tradizionali e ambienti cloud*, nei quali occorrerà gestire l'integrazione applicativa tra ambienti diversi, la sicurezza e la *privacy* di dati distribuiti su sistemi ibridi, il monitoraggio sull'uso delle infrastrutture e sui livelli di servizio erogati all'utente finale.

Occorre, in realtà, andare al di là della dimensione strettamente «verticale» della singola organizzazione, per comprendere come far dialogare i diversi attori dell'ecosistema, in modo da sviluppare una visione condivisa sulle diverse opportunità di approccio e strategie di servizio e trasformare il *cloud* nella piattaforma abilitante di un nuovo modello di infrastrutturazione della «pubblica amministrazione a rete».

2. Esperienze internazionali

L'analisi delle politiche e delle strategie dei paesi più preminenti, in Europa e in Asia, e degli Stati Uniti mostra come le iniziative, messe in atto dai governi per guidare il passaggio al *cloud computing*, abbiano subito un chiaro impulso negli ultimi due anni e non ci siano sostanziali segni di rallentamento nella direzione scelta: pur con politiche e approcci differenti, il settore pubblico si sta indirizzando verso il *cloud computing* principalmente, per lo meno in una fase iniziale, con un approccio tattico, finalizzato alla riduzione dei costi tecnologici.

Anche se gli Stati Uniti e alcuni paesi asiatici sono molto più avanzati e aggressivi nell'implementazione delle politiche volte all'adozione del *cloud* rispetto a quanto sviluppato dai paesi europei, che a loro volta non hanno un approccio uniforme e coeso sul tema, i paesi che stanno studiando e/o disegnando la loro politica di *government cloud* con maggior determinazione, considerano tutti l'Ict come infrastruttura critica del paese e come leva propulsiva per aumentare la produttività del sistema paese; inoltre si orientano verso l'adozione del *cloud computing* nella pubblica amministrazione concependolo come progetto sistemico di medio periodo, individuando precisi criteri di priorità nell'implementazione dei progetti. Se Regno Unito e Irlanda sembrano seguire il modello scandinavo, che tende a privilegiare più il controllo delle informazioni che la loro collocazione geografica, Germania, Francia, Spagna ed Italia si stanno orientando verso un approccio differente, orientato a garantire il mantenimento fisico dei dati all'interno dei confini, in alcuni casi investendo significativamente nella realizzazione di grandi *data center*, e a perpetuare un approccio regolamentare rigido e potenzialmente vincolante nei confronti dell'adozione di soluzioni *cloud*.

Sicuramente l'Asia, con i casi di Singapore e il Regno dell'Arabia Saudita, offre molti spunti di riflessione; i paesi in questione tuttavia sono delle realtà molto distanti da quella italiana per forma di stato, profilo geografico e sviluppo e governo dell'Ict nazionale: possono essere solamente una fonte d'ispirazione generale, ma con esperienze difficilmente riadattabili al contesto italiano; quello europeo, pur nella sua varietà, può essere una maggiore fonte di confronto:

– la Danimarca è uno dei paesi più avanzati per le iniziative in quest'ambito: il governo ha sviluppato un programma per l'adozione del *cloud computing* nella pubblica amministrazione mosso dai significativi risparmi economici possibili; nel documento strategico del 2010, la Danimarca si propone di sviluppare le infrastrutture necessarie per l'utilizzo di soluzioni di *cloud computing* e il settore pubblico è impegnato a fare da volano, avendo anche l'ambizione di divenire il caso di scuola per il *government cloud*;

– il Regno Unito ha sviluppato una delle strategie più ampie, denominata «*G-Cloud*», per l'adozione del *cloud computing* nella pubblica amministrazione, che è una delle priorità strategiche nell'agenda del governo Entro tre anni, il governo mira a tagliare del 35% il budget It, eliminando duplicazioni di tecnologia, e ottimizzando la condivisione di software e servizi; nell'approccio strategico Il governo aspira a diventare un «singolo acquirente intelligente» e svilupperà una procedura acquisti disegnata per facilitare la partecipazione delle Pmi ad appalti pubblici d'infrastruttura Ict. La strategia punta a limitare l'oligopolio delle grandi imprese nella fornitura d'infrastruttura It per la pubblica amministrazione, intervenendo anche sulle dimensioni dei contratti per renderli più flessibili, per aprire il mercato alle Pmi e a nuovi fornitori

– la Francia ha iniziato nel 2009 a sviluppare una strategia di *cloud* e, come parte di questo progetto chiamato «Andromeda», il governo sta collaborando con l'industria per costruire un data center nazionale e fornire hosting sicuro agli enti sia pubblici che privati;

– la Germania, con la strategia Ict 2015, sviluppata dal Ministro federale dell'economia, che considera l'Ict come infrastruttura critica del paese, ha definito il *cloud computing* come uno degli elementi fondanti lo sviluppo e la competitività del paese. Conseguentemente alla forma di stato federale, le strutture di governo dell'Ict sono fortemente decentrate: è stato creato un consiglio dei 16 Cio dei *Länder* per la standardizzazione e la pianificazione delle infrastrutture comuni e per la definizione delle linee guida e degli standard nella prospettiva dell'adozione del *cloud* nella pubblica amministrazione;

– dal 2008 il governo irlandese ha posto in essere un piano programmatico, «Smart Economy», in cui ha individuato la diffusione

dei servizi *cloud* negli enti pubblici come uno dei principali driver di crescita economica nel paese, con inoltre l'obiettivo di creare un numero significativo di nuovi posti di lavoro; punta inoltre a divenire «Centro europeo per il *cloud computing*» rivolto alla fornitura di servizi soprattutto al mondo delle aziende private;

– i Paesi Bassi hanno adottato una strategia per il *cloud computing* che lo pone come leva fondamentale per sostenere la produttività – a costi inferiori – delle amministrazioni, come un mezzo per sviluppare un approccio più efficiente al modo di lavorare.

Il *cloud computing* è certamente un fenomeno di mercato recente, che ha iniziato a svilupparsi nel settore privato ed è successivamente arrivato nel settore pubblico; la crisi finanziaria, l'interesse del settore privato e di alcune amministrazioni, come quella americana, stanno cercando di creare un ecosistema che contribuisca a che anche le amministrazioni pubbliche siano indotte ad adottare soluzioni tecnologiche basate sul *cloud computing*: tuttavia ad oggi non c'è un paese che abbia già sviluppato ed implementato completamente la «nuvola» nella pubblica amministrazione locale e/o centrale. Nonostante si sia in una fase ancora preliminare e che non sia ancora possibile identificare delle linee chiare tratte dai casi di successo o di fallimento nei paesi più avanzati, si evince che il vero punto critico, determinante per evitare il fallimento delle iniziative, non è tecnologico o finanziario, ma il modello di *governance* e l'approccio di sistema sul medio periodo, con l'individuazione di obiettivi chiari e di un sistema di controllo e responsabilità definito con precisione.

Dalle esperienze internazionali emerge chiaramente un modello organizzativo che tende all'accentramento della pianificazione strategica e finanziaria, alla gestione coordinata degli interventi posti in essere dalle realtà amministrative locali; all'interno delle scelte strategiche, dei finanziamenti erogati e dei controlli effettuati da una entità amministrativa deputata, gli enti amministrativi che implementano i progetti di *cloud* sono autonomi nella gestione operativa delle attività progettuali e dell'l'erogazione dei servizi. Il modello di governo che emerge dalle esperienze internazionali, può assumere varie forme dal Cio nazionale, con poteri d'indirizzo e di gestione, a struttura di garanzia con soli poteri di indirizzo e di controllo ma

senza capacitaà di intervento operativo, riflettendo anche le peculiarità del singolo paese: resta il fatto fondamentale che viene ovunque riconosciuta la necessità di un organismo nazionale deputato alla gestione del processo d'implementazione delle soluzioni *cloud* nelle pubbliche amministrazioni.

3. La Nuvola pubblica certificata come infrastruttura critica del Paese

Si è detto in precedenza che lo studio si focalizza principalmente sugli enti della pubblica amministrazione locale e che questi, per le loro caratteristiche, risultano utilizzatori di riferimento per soluzioni di *cloud pubblico*: questo modello (come illustrato nel Capitolo Primo), implica che i servizi, nelle diverse declinazioni IaaS, PaaS e SaaS, siano accessibili via internet e che i dati degli utenti (amministrazioni o aziende), che sono sottoposti alla normativa italiana ed europea sulla tutela dei dati personali, escano fisicamente dal perimetro informatico di sicurezza di diretta responsabilità dell'amministrazione o dell'azienda. La catena dei soggetti che contribuiscono all'erogazione di un servizio *cloud* può estendersi anche al di fuori dei confini del paese, fino a rendere difficile, o impossibile, per l'utente la localizzazione fisica dei propri dati: un rapporto contrattuale che apparentemente coinvolge solo tre soggetti (l'utente, *l'internet service provider* (Isp) e il *cloud cervice provider* (Csp)), può in realtà coinvolgere una catena difficilmente tracciabile di erogatori di servizi Isp e Csp appartenenti a giurisdizioni diverse. Nel quadro giuridico vigente, sia italiano che europeo, gli utenti di servizi *cloud* restano titolari dei dati, che tipicamente vengono memorizzati nei grandi *data center* dei *provider*, e mantengono l'intera responsabilità civile e penale delle violazioni di sicurezza, anche quando nel trattamento intervengono soggetti terzi su cui non hanno alcun controllo.

Appare quindi necessario introdurre un sistema di tutela verso i titolari dei dati che possono essere trasferiti nella nuvola, a garanzia che i servizi utilizzati rispettino i requisiti di sicurezza, di *privacy*, di accordi sui livelli di servizio, sulla localizzazione dei dati e sulle garanzie di portabilità: tale sistema è inequivocabilmente

quello della certificazione dei *provider*; si dovranno inoltre prevedere clausole contrattuali standard[1], accertare l'affidabilità finanziaria dei *provider* e quant'altro possa assicurare la conformità del loro operato alla normativa vigente, nazionale ed europea, in ambito di sicurezza e di tutela della *privacy*; ciò, a maggior ragione, quando si tratti di servizi *cloud* utilizzati da enti della pubblica amministrazione. È evidente che identiche considerazioni valgono anche per i fornitori di connettività internet, che pertanto dovranno essere certificati. Va osservato, a questo proposito, che le normative in merito non sono ancora disponibili, ma che è urgente emanarle, anche anticipando eventuali iniziative analoghe in sede europea.

La tecnologia permette di introdurre un nuovo tipo d'infrastruttura, una infrastruttura non «tangibile», cioè non costituita da oggetti fisici (strade, ponti, cavi, centrali) bensì da organizzazioni: l'insieme dei fornitori di servizi *cloud* e di servizi internet, che risulteranno certificati in base a norme e regolamenti tecnici italiani (da predisporre anche tenendo conto di eventuali analoghe iniziative in sede europea), costituisce di fatto una particolare infrastruttura Ict che, in quanto fattore abilitante l'utilizzo di servizi *cloud* con determinate requisiti e garanzie, è necessario considerare tra le infrastrutture critiche e strategiche del Paese; essa potrà essere realizzata e governata con modalità e strumenti che saranno approfonditi nei successivi paragrafi di questo capitolo; questa nuova infrastruttura, che rappresenta una realtà astratta, nel seguito sarà chiamata Nuvola pubblica certificata**:** pubblica perché la rete utilizzata è internet (e quindi si tratta di un *public cloud* secondo la definizione Nist) e certificata perché i servizi *cloud*, singolarmente certificati, sono accessibili attraverso internet provider a loro volta certificati.

La Nuvola pubblica certificata è definita quindi, in termini di modello concettuale, come: *l'insieme organizzato di fornitori di servizi cloud (Csp) e di fornitori di servizi di connettività internet (Isp) che hanno ottenuto la certificazione di sicurezza in conformità alla normativa e ai regolamenti tecnici italiani*.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:-0005:0018:EN:PDF.

Così definita la Nuvola pubblica certificata è un'infrastruttura aperta in quanto non pone alcuna restrizione sulla natura giuridica dei *provider*, o relativa al contesto giuridico nel quale i *provider* operano e realizzano i servizi, ma richiede che, qualora questi eroghino servizi ad una utenza che opera nel contesto giuridico italiano siano in grado di garantire di essere stati certificati (anche presso organismi non nazionali) secondo la normativa italiana (o eventualmente europea) vigente. Questa infrastruttura Ict di servizi certificati in cui i *cloud provider*, soprattutto se erogano servizi di tipo IaaS, sono in genere dotati di grandi *data center*, è funzionale non solo alle esigenze dalle pubbliche amministrazioni, ma anche a quelle delle imprese, grandi, medie e piccole, anch'esse soggette alla normativa sulla sicurezza e sul trattamento dei dati personali.

La caratterizzazione dei *provider* può essere diversa in funzione dei modelli di servizio erogati (IaaS, PssS o SaaS), attualmente i *cloud service provider* accessibili via internet sono, nella maggior parte dei casi, aziende internazionali che utilizzano *data center* consolidati di grandi dimensioni collocati al di fuori del territorio nazionale. Nulla ovviamente impedisce che possano operare anche sul territorio nazionale qualora esistano le condizioni di economicità del servizio e di ritorno dell'investimento. Peraltro anche soggetti pubblici italiani, soggetti privati italiani a partecipazione pubblica o anche soggetti privati italiani potrebbero avere interesse ad operare come Csp certificati sulla Nuvola pubblica certificata; va osservato inoltre che nelle condizioni attuali del mercato, gli Isp sono tipicamente soggetti privati locali che, nella prospettiva delineata, dovranno garantire una connettività adeguata, in termini di banda, sicurezza ed efficienza, tra gli utenti e i Csp e pertanto dovranno ugualmente rispondere a precise normative ed essere certificati.

La Nuvola pubblica certificata si è definita come una *cloud pubblica* aperta, in quanto i servizi sono accessibili via internet, sia pure con il vincolo di utilizzare *provider* certificati; gli utilizzatori della nuvola saranno tipicamente piccole e medie imprese e, nel campo di specifico interesse di questo studio, tutte le pubbliche amministrazioni medie e piccole. Le grandi organizzazioni, private e pubbliche, seguiranno probabilmente un altro percorso, evolvendo inizialmente verso soluzioni in *cloud privato*, che comporta prima di tutto

il consolidamento dei rispettivi *data center* e, successivamente o contemporaneamente, potranno fare accesso anche a servizi di *cloud pubblico* realizzando soluzioni di *cloud ibrido*.

Questa impostazione concettuale non impedisce di riservare alcuni servizi *cloud* certificati a particolari categorie di utenti (per esempio ai comuni o alle scuole o anche a tutte le pubbliche amministrazioni) realizzando così anche la possibilità di costruire una o più *nuvole di comunità* che insistono sulla Nuvola pubblica certificata. È importante a questo punto precisare che i servizi *cloud*, anche quelli di tipo SaaS, hanno natura completamente diversa dai *servizi applicativi* previsti dal Cad, che sono servizi istituzionali che le amministrazioni certificanti devono a norma di legge rendere disponibili alle amministrazioni procedenti attraverso la *cooperazione applicativa*; allo stato dell'arte della sicurezza delle reti, se si prescinde da questioni regolamentari, anche questi servizi di natura intrinsecamente diversa potrebbero essere esposti sulla Nuvola pubblica certificata, per consentire l'integrazione tra i sistemi di *back end* delle pubbliche amministrazioni.

Si è detto come la Nuvola pubblica certificata sia un'infrastruttura critica e strategica: per tale motivo dovrà esserne assicurata la stabilità e la continuità nel tempo: ciò richiede una struttura permanente che ne gestisca la realizzazione, l'evoluzione e la sostenibilità in un'ottica sistemica. Come ogni infrastruttura strategica e critica è necessario dotare la Nuvola pubblica certificata di un organo di governo dotato di strumenti adeguati di tipo normativo, organizzativo e tecnico che tengano conto delle sue peculiarità, ed è necessario verificare se questi strumenti esistano eventualmente già nel quadro istituzionale vigente oppure vadano creati.

La Nuvola pubblica certificata è definita come un sistema organizzato di Csp e di Isp certificati, governato da una struttura capace di coordinare l'attività di soggetti distinti e autonomi che in modo coordinato devono svolgere, ciascuno per la parte di competenza, i seguenti compiti:

1. predisporre norme e regolamenti che, prendendo atto delle possibilità del *cloud computing*, istituzionalizzino i soggetti attori della Nuvola pubblica certificata (vedasi il Capitolo Primo);
2. definire gli standard necessari tecnici, di sicurezza, contrattuali e di affidabilità dei provider; la standardizzazione è l'aspetto più rilevante, in quanto consente agli utenti di accedere a servizi equivalenti erogati da *provider* diversi (quindi garantisce una vera concorrenza tra i *provider*) e soprattutto garantisce la possibilità di migrare da un *provider* all'altro;
3. realizzare e gestire alcune infrastrutture tecnologiche minime essenziali per:
    a. registrare, in un apposito elenco, i Csp e gli Isp certificati che lo richiedono (accreditamento);
    b. consentire agli utenti di reperire i servizi certificati disponibili;
    c. identificare a livello nazionale o europeo gli enti terzi qualificati per effettuare la certificazione di Csp e Isp;
    d. attribuire a selezionati organismi terzi di *auditing*, il compito di verificare periodicamente il rispetto, da parte dei *provider* della Nuvola pubblica certificata, dei requisiti di certificazione e di accreditamento;
4. definire criteri e logiche di certificazione anche secondo il grado di sicurezza dei servizi (non tutti potranno avere lo stesso grado di sicurezza), definendo eventualmente criteri di affidabilità crescenti, in funzione della rilevanza sistemica ed economica del servizio erogato, ad esempio secondo un modello cooptato dal modello di qualificazione dei fornitori in ambito Cmmi (*Capability maturity model integration*), siffatto:
    a. massimo livello di affidabilità e tutela per i Csp eroganti servizi con impatti di sicurezza o comunque potenzialmente bloccanti per il sistema, con specifici requisiti operativi e di sicurezza definiti su base strategica e quindi a livello normativo;
    b. livello intermedio per servizi ad alto impatto ma non bloccanti, con elementi di affidabilità definiti ancora a livello regolamentare nazionale;
    c. livello operativo ordinario per Csp eroganti servizi a supporto delle attività ordinarie della pubblica amministrazione, qualificati sulla base di standard di mercato (specifiche ISO, piuttosto che livelli di certificazione Cmmi).

3.1. Aspetti normativi

Con riferimento al quadro normativo vigente e ai compiti oggi assegnati alle strutture esistenti, è prima di tutto necessario istituzionalizzare nel Codice dell'amministrazione digitale il ruolo di *cloud service provider* certificato e di *cloud identity provider*, in modo simile a quanto avviene per i certificatori di firma elettronica agli art. 26, 27 e 29. I fornitori, pubblici o privati, che aspirano a fornire servizi alla pubblica amministrazione dovranno ottenere, a proprie spese, una certificazione presso enti terzi qualificati, secondo criteri e regole tecniche predisposte dal Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica e da DigitPA, in modo che le amministrazioni, ma anche le imprese utenti, siano automaticamente garantite di ottenere servizi conformi a norme e regolamenti tecnici e contrattuali. Il ruolo di *cloud auditor* deve invece essere ricoperto da soggetti che possano garantire l'indipendenza che è necessaria per una credibile struttura di *auditing*, secondo gli standard internazionali (si vedano le specifiche Isaca per il ruolo degli *auditor* Is certificati Cisa). Va inoltre osservato che, in particolare per le funzioni di *auditing* nel contesto della pubblica amministrazione, l'indipendenza e la terzietà dell'*auditor* risultano particolarmente rilevanti e potrebbero orientare verso il modello standard di mercato, basato su strutture di professionisti certificati secondo gli standard internazionali. DigitPA nell'ambito di una rivisitazione dei suoi compiti potrebbe, ad esempio, svolgere il ruolo di stazione appaltante per le attività di progettazione e gestione delle infrastrutture tecnologiche necessarie per supportare la Nuvola pubblica certificata e per l'attribuzione, a soggetti qualificati, dei compiti di *auditing*, compiti che sono analoghi a quelli che attualmente svolge nel contesto Spc e Spcoop.

Oggi in mancanza di un quadro di riferimento istituzionale e organizzativo che caratterizzi i servizi della Nuvola pubblica certificata appare giustificata le posizione di chi – e giustamente in prima linea l'Autorità Garante – suggerisce, in relazione agli aspetti di sicurezza e di tutela della privacy, estrema cautela nell'uso dei servizi *cloud* che sono attualmente accessibili via internet. Nella legislazione vigente (Cad e Codice della privacy) esistono – non solo per le pubbliche amministrazioni, ma per tutti i privati titolari di dati personali – vincoli normativi di sicurezza e di responsabilità sui dati che hanno suggerito all'Autorità di produrre il documento *Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*, allegato alla Relazione 2010 del Garante al Parlamento. Questo documento fornisce undici argomentati suggerimenti per gli utilizzatori del *cloud* in tema di sicurezza, livelli di servizio, clausole contrattuali e necessità di accertare l'affidabilità anche finanziaria del *provider*, raccomandazioni che comportano, da parte degli utilizzatori, complesse verifiche normative, tecniche e contrattuali e di affidabilità nei riguardi dei fornitori di servizi *cloud*. Allo stato delle cose per utilizzare con relativa tranquillità i servizi *cloud pubblici* le singole amministrazioni e le imprese dovrebbero svolgere in proprio e a costi propri queste verifiche: si tratta di adempimenti tecnicamente complessi e costosi, che vanno spesso al di là delle capacità di soddisfarli della maggior parte dei soggetti destinatari; il risultato, sicuramente non voluto, è però quello di scoraggiare i piccoli e medi utenti, che massimamente potrebbero beneficiarne, dall'adottare servizi *cloud* pubblici che già oggi sono offerti sul mercato.

La sicurezza informatica e la tutela della *privacy* costituiscono, per le amministrazioni e le aziende, un costo che tende ad essere indipendente dalla loro dimensione economica. Il legislatore, finora, ha perlopiù dettato principi generali, applicabili a tutti indistintamente. In futuro sarà opportuno prevedere regole e direttive diversificate, dunque più «sostenibili», per quanto riguarda gli adempimenti di sicurezza (inclusa la tutela della *privacy*). Occorre tener conto dei costi e delle dimensioni dell'amministrazione o dell'azienda, accettare un ragionevole margine di rischio e considerare non solo la tipologia del dato, ma anche il suo valore economico. Tuttavia proprio il *cloud computing* può offrire la possibilità di fornire alle amministrazioni questo tipo di servizi, a costi sopportabili e senza richiedere investimenti, diventando quindi una tecnologia abilitante per consentire alle piccole amministrazioni, e anche alle piccole imprese, di adeguare i propri sistemi informativi alle norme sulla sicurezza, sempre che abbiano accesso a una banda internet adeguata.

4. La sicurezza strategica dei dati

Per comprendere le innovazioni possibili e i risparmi che si potrebbero realizzare proponendo alcuni vincoli normativi in modo più sostenibile, è necessario andare al cuore del problema: i dati e la loro sicurezza.

Storicamente i dati operazionali, quelli che sono necessari allo svolgimento dei compiti di servizio (altri dati sono raccolti a fini decisionali o statistici) venivano conservati su supporti fisici cartacei utilizzabili senza alcuna mediazione. Oggi i dati operazionali delle amministrazioni sono conservati in modo codificato in forma elettronica e sono utilizzabili solo attraverso la mediazione di un sistema informatico. L'adozione di servizi *cloud* di tipo IaaS consente sia di spostare i dati nel *cloud* acquisendo servizi di *storage* sia di utilizzare *server* virtuali dove poter eseguire le proprie applicazioni. A questo punto è naturale chiedersi: dove sono i dati e di chi sono i dati?

Finora, per ragioni storiche comprensibili, ha prevalso nella normativa l'idea che i dati operazionali sono di chi ha il compito istituzionale di raccoglierli, certificarli (cioè dichiararli autentici), conservarli e utilizzarli per lo svolgimento dei propri compiti di servizio. Si tratta tuttavia di una visione che va ormai considerata inadeguata. Una visione più aderente alla realtà tecnologica odierna, potrebbe ipotizzare che i dati delle amministrazioni sono *res publica* e sono semplicemente affidati alle amministrazioni e agli enti dello stato, alle regioni, alle province ed ai comuni per fini specifici, e con responsabilità specifiche e differenziate (anche perché spesso i dati di un'amministrazione devono essere utilizzati nei procedimenti di un'altra).

È una realtà di fatto, soprattutto nel contesto del *cloud computing*, che i dati non hanno più un unico vero responsabile della sicurezza, ma esiste una molteplicità di soggetti che possono esercitare responsabilità di sicurezza diverse sugli stessi dati e in momenti diversi. La normativa vigente è invece nata in un mondo senza reti e deriva da una cultura senza reti: il sistema informativo di ogni organizzazione conserva procedure e dati in un luogo fisicamente circoscritto, nell'illusione che così siano più sicuri e che le responsabilità sulla loro sicurezza più oggettivabili. Se però ci si richiama alla cultura della rete e del *cloud* e si cerca di beneficiare dei servizi IaaS, ad esempio di utilizzare servizi di *storage* o di *disaster recovery* offerti in rete da un *cloud provider*, si deve affrontare una situazione più complessa, in cui il sistema informativo di un'organizzazione (composto da apparecchiature, procedure e dati) in pratica si smaterializza nella nuvola e le sue funzionalità sono garantite da una molteplicità di soggetti: in un simile contesto, al di là delle garanzie sulla qualità e i livelli di servizio, il tema veramente critico è quello della sicurezza dei dati.

Tralasciando di considerare i temi relativi alla *sicurezza fisica* degli impianti, ad esempio la protezione da eventi catastrofici, in quanto sono comuni alla sicurezza fisica di qualunque infrastruttura strategica del Paese, occorre focalizzare l'attenzione sugli aspetti che caratterizzano la *sicurezza informatica*, che si declina su vari piani e, soprattutto, concentrarsi sugli aspetti che riguardano la sicurezza dei dati, che costituiscono il vero patrimonio di un ente e non devono essere persi o alterati.

In un contesto di rete e di *cloud* i dati possono essere movimentati e conservati da soggetti giuridici diversi da quelli che li hanno generati e che li devono utilizzare per erogare i propri servizi istituzionali; si pensi ad esempio ad un comune che acquisisce un *server* virtuale e capacità di memorizzazione per svolgere le proprie funzioni anagrafiche: i soggetti coinvolti sono il comune, il suo *internet service provider*, che assicura la connettività, e il *cloud service provider* che assicura il servizio di virtualizzazione e *storage*; pensando ad un piccolo comune o a una piccola azienda, è certo che il livello di sicurezza che può ottenere utilizzando la nuvola è enormemente superiore al livello di sicurezza che potrebbe gestire in proprio, date le risorse materiali ed umane che i provider possono mettere in campo, incomparabili con quelle che potrebbero mettere in campo il comune o l'azienda.

Per quanto riguarda il trattamento dei dati è possibile individuare numerose responsabilità, oggettivamente distinte:

– responsabilità di raccogliere dati *autentici* e di certificarli; a questo proposito va fatta un'importante osservazione: un corretto modello amministrativo dovrebbe garantire che un solo ente abbia la responsabilità di raccogliere un determinato tipo di dati e di cer-

tificarli nei confronti di chi ne ha bisogno per svolgere i propri procedimenti, ma ciò purtroppo non è sempre vero, con i conseguenti problemi di qualità dei dati, quali duplicazioni errate e altri inconvenienti simili con pesanti ripercussioni sul piano dell'efficienza dell'azione degli enti;

– responsabilità di garantire l'*integrità* dei dati, cioè che i dati, una volta raccolti, possano essere modificati solo da soggetti autorizzati, sia quando siano memorizzati localmente sia quando vengano trasferiti in rete; ogni violazione dell'integrità, locale o nel trasferimento in rete, deve essere rilevabile;

– responsabilità di garantire la *confidenzialità*, cioè che il dato possa essere conosciuto solo da soggetti autorizzati;

– responsabilità di garantire la *disponibilità* del dato, cioè la garanzia che il dato sia sempre accessibile, o venga recuperato in tempi certi, sia a fronte di eventi criminali che di eventi naturali catastrofici o di guasti.

Questi sono i tipici parametri su cui si misura e si costruisce la sicurezza informatica e risulta evidente, nell'esempio fatto in precedenza, che il titolare del comune può esercitare direttamente la responsabilità di garantire l'autenticità del dato, mentre l'Isp ha, nei fatti, le responsabilità della integrità e della confidenzialità durante la trasmissione, e il Csp ha la responsabilità della disponibilità, dell'integrità e della confidenzialità, ottenuti tipicamente con strumenti crittografici e, soprattutto, con il controllo dell'accesso (cioè con il riconoscimento degli addetti autorizzati). È chiaro che si è di fronte a materia contrattuale giuridicamente molto complessa, che però non si risolve mantenendo semplicemente le cose come stanno, lasciando la responsabilità totale in carico all'anello più debole della catena e meno coinvolto negli aspetti critici della sicurezza, che, nell'esempio fatto, è il comune.

Il controllo dell'accesso comporta l'esistenza, nella Nuvola pubblica certificata, di un sistema nazionale federato di gestione dell'identità personale degli utenti e delle loro qualifiche e ruoli e deleghe, per poter assegnare e gestire le opportune autorizzazioni all'accesso. Si tratta, in pratica, di porre in esercizio un sistema di *identity management federato*, secondo modelli ormai collaudati e

comunemente diffusi a livello internazionale e già parzialmente adottati anche da alcune regioni italiane; per questo è necessario che, nella Nuvola pubblica certificata, sia presente una particolare categoria di service provider, i *cloud identity provider* (Cip) a loro volta soggetti certificati, con il compito di rilasciare agli altri servizi *asserzioni certificate* (basate su standard internazionali) sull'identità personale di chi accede ai servizi e sugli attributi necessari per concedere l'autorizzazione all'accesso. In particolare i Cip sono anche i soggetti incaricati di gestire il processo di *provisioning* delle credenziali agli utenti. (Per una discussione completa sugli aspetti di gestione dell'identità federata si veda il documento riportato all'Appendice 3).

Gli utenti privati (le imprese) non hanno l'obbligo di utilizzare servizi certificati, probabilmente più costosi, ma in questo caso si dovranno assumere direttamente le responsabilità relative agli adempimenti di sicurezza e di tutela della *privacy*; per gli enti della pubblica amministrazione è necessario invece rendere obbligatorio l'accesso a servizi certificati, a garanzia dell'adempimento degli obblighi relativi all'accertamento dell'affidabilità tecnica, giuridica e finanziaria del *provider*.

Quanto si è sviluppato sul tema della sicurezza dei dati fa emergere un altro aspetto critico, strettamente legato al cambio di paradigma introdotto dalle possibilità offerte dalle nuove soluzioni tecnologiche: vi è cioè una precisa necessità che il decisore politico-istituzionale identifichi ed enumeri con precisione le basi dati strategiche per il funzionamento del Paese, quelle cioè che sarà necessario mettere in sicurezza consolidandole in opportuni *data center* e, tra esse, identificare quelle che, per ragioni di sicurezza nazionale, debbano essere mantenute in *data center* operanti entro i confini nazionali. A questo proposito va osservato come la pubblica amministrazione italiana, a livello centrale e locale, disponga di numerose decine di *data center*, alcuni gestiti ancora con tecniche e procedure obsolete, quindi necessariamente costosi e poco efficienti: una strategia di migrazione verso il *cloud* rappresenta anche un'occasione per rivedere la situazione esistente, con l'obiettivo di razionalizzare, consolidare e modernizzare i sistemi informativi, invece di procedere a costosi investimenti al solo fine di fare fronte all'ob-

solescenza delle dotazioni tecnologiche, senza apprezzabili vantaggi sul piano applicativo e funzionale.

5. La transizione verso il *cloud computing*

Il processo di migrazione verso il *cloud computing* da parte delle amministrazioni pubbliche sarà necessariamente graduale, si svolgerà secondo diversi modelli architetturali, mantenendo l'integrazione e la compatibilità con i servizi esistenti: le strategie seguite potranno essere rivolte all'uso di servizi di *cloud pubblici* in particolare della Nuvola pubblica certificata, oppure al consolidamento dei propri *data center* in *cloud privati, ibridi o di comunità*.

Per governare la transizione, è necessario un censimento dei *data center* attualmente operativi e una pianificazione accurata, che includa una *roadmap* di transizione, un prospetto di costi e benefici economici e funzionali e – se possibili – incentivi per favorire l'aggregazione dei *data center* esistenti; nel caso in cui i *data center* appartengano ad enti locali che svolgono gli stessi compiti istituzionali ed erogano gli stessi servizi, si dovrebbe incentivarne la standardizzazione per favorire un consolidamento anche a livello applicativo. Nel censimento potrebbero rientrare anche i *data center* di grandi enti pubblici e imprese a partecipazione pubblica (nazionale e locale), spesso dotati di elevate capacità e potenza di calcolo, superiori a quelle effettivamente utilizzate e facilmente espandibili; come già osservato tutte le infrastrutture critiche nazionali (gasdotti, oleodotti, elettrodotti, ferrovie, autostrade, poste, telecomunicazioni, ecc.) sono oggi totalmente dipendenti dalle tecnologie Ict; è presumibile che i soggetti che le gestiscono possiedano *data center* capaci di evolvere, nel quadro di una partnership pubblico-privata ben costruita, verso l'offerta di servizi *cloud*, partecipando così, come fornitori di servizi, alla Nuvola pubblica certificata, infrastruttura Ict strategica del Paese aperta a tutti. Si potrebbero anche valorizzare altri *asset* significativi per il sistema già presenti nel paese e comunque vincolati, per prassi interne o per obblighi regolamentari, a logiche di *governance* misurabili (come ad esempio nel mondo bancario), con ciò abilitando la realizzazione di una infrastruttura, anch'essa con natura giuridica da definire[2], che potrebbe avere anche natura privata. Ciò in base a due considerazione:

– il mercato dei *cloud provider* richiede la presenza di un abilitatore forte, capace di avviare i primi progetti focalizzandosi più sugli aspetti sistemici che su quelli commerciali, aprendo così il mercato almeno a livello di infrastrutture e abilitando anche alcuni elementi propedeutici ai servizi *cloud* veri e propri. Si pensi ad esempio alle grandi infrastrutture *Multi protocol label switching* (Mpls) detenute dai grandi *data center* nazionali;

– grandi realtà private con valore sistemico per il paese hanno, da sole, tutte le potenzialità per abilitare pienamente tutti i servizi IaaS e PaaS necessari per lo *start up* operativo ed efficace di una politica *cloud* nazionale: è sufficiente fare riferimento alle capacità Ict detenute, nel settore dell'energia e delle utilities, da Eni a Enel a Terna, realtà considerate critiche per il loro valore sistemico e quindi avviate, anche per normativa primaria, a un percorso di controllo regolamentare; oppure a quelle detenute dai primari istituti bancari, si pensi ad esempio ai centri servizi di Intesa San Paolo o di Unicredit o al Consorzio Mps, anch'essi già considerati a valore sistemico e posti sotto controllo sia per normativa primaria sia per prassi regolamentare nazionale e internazionale.

La realizzazione di una realtà di *partnership*, fondata su questi contesti operativi porterebbe diversi vantaggi:

– capitalizzerebbe su scala nazionale competenze e *asset* già presenti, ma di fatto non qualificati in un quadro sistemico;

– permetterebbe la costituzione di un contesto aziendale privato che potrebbe supportare, non solo operativamente ma anche giuridicamente, un ente con funzioni di controllo analoghe a quelle che Banca d'Italia esercita sul sistema bancario;

– indirizzerebbe il mercato del *cloud* senza richiedere fin dall'inizio pesanti investimenti e senza creare situazioni monopolistiche, sia perché si tratterebbe di attori che non operano nel mercato Ict sia perché si porrebbero in un quadro regolamentare controllato da

[2] In questo caso esistono minori riferimenti in termini di modelli o di prassi, gli stessi centri servizi bancari operano con una logica di segmentazione verticale.

un ente esterno;

– faciliterebbe una visione integrata delle componenti critiche del sistema Paese, coerentemente con le indicazioni dell'Unione europea, che progressivamente dovranno essere effettivamente recepite anche in Italia;

– permetterebbe ai *Cloud Providers* italiani di focalizzarsi sui servizi a valore aggiunto SaaS e BPaaS, svincolandoli dalla componente IaaS che, necessitando di grandi infrastrutture, sarebbe sempre tendenzialmente offerta da pochi grandi attori internazionali, che però avrebbero la barriera all'accesso rappresentata dalla eventuale esigenza di mantenere almeno i servizi critici in Italia; i provider italiani si potrebbero così focalizzare sulla componente servizi SaaS, più facilmente perseguibile, probabilmente con maggiori margini e con maggiore valore percepito anche per gli utenti, permettendo da subito di realizzare portafogli servizi di notevole ampiezza;

– garantirebbe gli utenti riguardo a esigenze normative o culturali relative al mantenimento delle componenti critiche su infrastrutture sotto diretto controllo nazionale.

Il modello risulterebbe architetturalmente sostenibile anche in considerazione dei recenti investimenti operati, dai grandi attori del mercato, su grandi progetti di consolidamento, virtualizzazione e IaaS, o del modello architetturale già presente in realtà con grandi *cluster* geografici basati su infrastrutture consolidate su reti Mpls in ambito nazionale o europeo.

6. I progetti nazionali a valenza sistemica

L'evoluzione tecnologica verso il *cloud computing* secondo il modello proposto mostra l'urgenza di adeguare la normativa italiana vigente (congelata in una norma primaria come è il Cad o anche il d.lgs. 196/2003, derivato da una normativa europea ormai vecchia). In molti casi, pur prescindendo dalla tecnologia *cloud*, è inadeguato il modo con cui il legislatore affronta i temi della sicurezza, con soluzioni tecniche e organizzative di tipo puramente prescrittivo, che le amministrazioni, nella stragrande maggioranza, non potranno rispettare per mancanza di competenze e di risorse. Il modo, in cui il legislatore italiano affronta questi temi, prescinde dal fatto che le amministrazioni pubbliche non sono tutte uguali in termini di dimensioni economiche e di competenze Ict: non vengono in genere messe a disposizione le risorse necessarie o predisposti servizi atti a facilitare gli adempimenti. trascurando gli impatti economici delle prescrizioni.

Per meglio comprendere quanto si afferma è utile descrivere un caso davvero emblematico. La necessità sistemica di mettere in sicurezza i dati operazionali, così frammentati di ogni amministrazione centrale o locale mediante procedure di *back-up*, *disaster recovery* e continuità operativa, è ovviamente incontestabile: ma un articolo di legge non crea tuttavia automaticamente un «progetto sistemico» che raggiunga lo scopo in tutto il paese. È esempio di cattiva pratica legislativa, ad esempio, l'integrazione recentemente introdotta nel Cad con l'art. 50-bis – *Continuità operativa*[3] e l'art. 51 – *Sicurezza*

[3] Art. 50-*bis* – *Continuità operativa*. 1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di *disaster recovery*, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di *disaster recovery* delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni, che lasciano l'onere di tutti gli adempimenti previsti sulle singole amministrazioni (si ricordi che il Cad si applica anche a tutte le amministrazioni locali in particolare ai circa 7.500 comuni che hanno meno di 20.000 abitanti e ai quasi 6.000 comuni che hanno meno di 5.000 abitanti, si applica ad alcune centinaia di Asl, il cui numero varia in continuazione, e agli istituti scolastici che sono circa 14.000, ecc.). Al di fuori della normativa sulla tutela dei dati personali, una simile prescrizione generale sulla sicurezza effettivamente mancava e il principio è perfettamente condivisibile: infatti è sicuramente nell'interesse del Paese che non vengano persi dati essenziali al funzionamento della macchina amministrativa. Ma non è ragionevole ritenere che ogni piccolo comune o ogni scuola possa, singolarmente, assicurare la continuità operativa e il *disaster recovery*, senza avere a disposizione adeguate competenze, tecniche ed organizzative, per dare esecuzione a obblighi di legge di questa complessità e per predisporre i necessari studi di fattibilità. Se fossimo in presenza di *provider* certificati non avrebbe senso richiedere a tutte le amministrazioni di svolgere dettagliati studi di fattibilità da sottoporre al parere di DigitPA, che sarebbe sommerso da decine di migliaia di studi. Tra l'altro è importante considerare che il costo di adeguamento a queste, come a numerose altre norme del Cad, non è proporzionato ai loro parametri dimensionali e molte amministrazioni sono nella pratica impossibilità di rispettare gli adempimenti anche nei casi in cui le norme rispondono a finalità d'interesse generale per la sicurezza del Paese. Quello citato è solo uno degli esempi, il più recente, di un «malcostume» legislativo che detta norme praticamente inattuabili e magari prevede, a discrezione degli interessati, la possibilità di sottrarsi all'adempimento perché «il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche»; d'altronde il Cad è pieno di norme di questo tipo, basti pensare alle norme sulla carta d'identità elettronica e sull'accesso ai servizi in rete, che non sono attuate da oltre dieci anni e che

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

inoltre sono praticamente impossibili da attuare.

Per assicurare l'omogeneità delle soluzioni scelte dalle singole amministrazioni sarebbe più logico assegnare esplicitamente, al Ministro delegato, il compito di costituire un ente di standardizzazione dei dati e dei servizi della pubblica amministrazione e di identificare il Sistema di certificazione che di fatto consenta ai fornitori una omologazione dei servizi, rendendo poi obbligatorio per le amministrazioni l'uso di servizi certificati. L'esigenza di un ente di standardizzazione emerge continuamente ed è stata segnalata da anni da tutti gli esperti: il messaggio forse è arrivato, ma non è sufficiente limitarsi a elencare il tema tra i compiti del Dipartimento dell'innovazione e della funziona pubblica (d.m. 13 luglio 2011): *Riorganizzazione del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica*[4].

Questo studio, utilizzando il *cloud computing* come facilitatore, si propone di affrontare i singoli temi nella forma di progetti nazionali di valenza sistemica, utilizzando i servizi della Nuvola pubblica certificata, che offra un numero di servizi infrastrutturali IaaS già disponibili sul mercato e con adeguati incentivi alle amministrazioni per raggiungere rapidamente il risultato desiderato, nell'ambito di un piano concordato che le coinvolga tutte. Si deve precisare che l'esigenza di progetti di natura sistemica è preesistente alle tecnologie di *cloud computing*: si presenta comunque anche nel caso di progetti d'integrazione e cooperazione applicativa, che non si è realizzata finora proprio per la mancanza di adeguati modelli e strutture di gestione progettuale a livello sistemico. Costruendo la Nuvola pubblica certificata, così come discussa, lo Stato passa da un atteggiamento puramente prescrittivo, che abbandona le amministrazioni a sé stesse senza finanziarne i costi, ad un atteggiamento di servizio, in cui mette a disposizione gli strumenti per soddisfare le esigenze di sicurezza del sistema paese; attraverso la pratica della certificazione dei *provider* lo Stato creerebbe un sistema in grado di offrire agli utilizzatori la garanzia che i servizi erogati sono conformi alle norme di sicurezza e di tutela della *privacy*, sollevandoli quindi

[4] G.U. n. 224 del 26 settembre 2011.

dal compito di verificare, in proprio, la rispondenza dei servizi utilizzati ai requisiti tecnici, contrattuali e di affidabilità del *provider*.

Questo approccio consente di pensare al *cloud computing*, ed in particolare alla Nuvola pubblica certificata, come ad una infrastruttura strategica abilitante e strumentale per consentire lo sviluppo di *cluster* di progetti nazionali di valenza sistemica, ciascuno dotato di una propria legge istitutiva e di un proprio budget pluriennale, per consentire a tutte le amministrazioni coinvolte, soprattutto alle più piccole, ma anche alle imprese (che per quanto riguarda il trattamento dei dati personali hanno obblighi analoghi derivanti dal d.lgs. 196/03), di adeguarsi più facilmente e con costi minori a norme e regole tecniche che altrimenti sarebbero disattese. Si considerano progetti a valenza sistemica tutti i progetti che coinvolgono amministrazioni centrali e locali, e in particolare tutte le amministrazioni locali che esercitano le stesse funzioni istituzionali su territori diversi: l'obiettivo dei questi progetti è creare, in un arco di tempo pianificato e ragionevole, una situazione omogenea rispetto alla disponibilità e alla qualità degli stessi servizi pubblici erogati in tutte le aree del Paese, contribuendo così a realizzare la coesione sociale.

Possono essere individuati numerosi progetti nazionali di natura sistemica, che comportano azioni pianificate, gestite e coordinate temporalmente di tutte le amministrazioni coinvolte nel raggiungimento di un obiettivo collettivo predefinito e per questi, senza costi eccessivi, si potrebbero avviare gradualmente almeno gli studi di fattibilità: è evidente che l'individuazione dei progetti e la loro priorità è una decisione eminentemente politica.

In tema di progetti nazionali a valenza sistemica è necessario fare un'ultima precisazione: contrariamente a una convinzione molto diffusa, il *cloud computing* non risolve i problemi di integrazione tra sistemi informativi, delle amministrazioni, tuttavia ne è un forte abilitatore perché favorisce la standardizzazione delle soluzioni. Per affrontare questi problemi è stato realizzato il *sistema pubblico di connettività e cooperazione*, che tuttavia non ha dato visibili risultati pratici. Anche in questo caso, procedendo per progetti mirati di valenza sistemica, si potrebbero ottenere, in un ragionevole arco di tempo, quei risultati da sempre auspicati in ogni piano di e-government e mai raggiunti, come ad esempio ottenere servizi da un'amministrazione senza dover presentare informazioni e documentazione già in possesso di altre amministrazioni: ciò che sempre più irriterà i cittadini nativi digitali, che ormai possono ottenere direttamente via *web* queste informazioni, è il fatto che le stesse informazioni non possano essere ottenute automaticamente del sistema informativo della amministrazione che le richiede.

7. La *governance* dei progetti a valenza sistemica

I progetti di natura sistemica sono estremamente complessi (spesso non dal punto di vista tecnico) perché coinvolgono tutte le amministrazioni del Paese che erogano su territori diversi uno stesso servizio. Il fascicolo sanitario elettronico (Fse) di cui si è trattato approfonditamente è un tipico progetto di natura sistemica che in questo momento molte regioni stanno realizzando, in modo sostanzialmente indipendente l'una dall'altra, sia pure con la dichiarata intenzione di integrare i propri sistemi, per ottenere un servizio a livello nazionale che offra al cittadino, ma soprattutto agli operatori sanitari ai quali il Fse è principalmente destinato, una visione integrata dei dati medici, indipendentemente dalla regioni in cui il cittadino stesso è stato curato. Tuttavia i dati sanitari sono generati dalle aziende sanitarie regionali (Asr), non l'ente regione e, data l'alta mobilità, voluta o accidentale, dei cittadini che possono essere ricoverati e curati in regioni diverse, vi è l'elevato rischio che sarà quasi impossibile realizzare l'aggregazione dei vari fascicoli in un fascicolo sanitario unico nazionale, in cui siano integrati i dati del cittadino indipendentemente da dove sia stato curato. Il risultato auspicato non può nascere da comitati o da commissioni interregionali, anche se si accordassero ipoteticamente sulle architetture e sugli standard. Il risultato può solo essere il prodotto di un «progetto» nazionale.

Ogni progetto a valenza sistemica nazionale deve essere caratterizzato da:

– uno studio di fattibilità;

– una legge istitutiva che allochi un budget pluriennale e definisca gli obblighi delle amministrazioni coinvolte e le modalità di finanziamento delle stesse;

– un disegno architetturale;
– un progetto e da un piano di sviluppo informatico;
– una struttura di project management;
– una strategia di sostenibilità a regime.

Dovranno essere presidiate le due dimensioni sotto indicate:
– una dimensione organizzativa, che preveda un'articolazione su più livelli del modello, a livelli di delega potenziale e distribuzione organizzativa crescenti:
  – definizione di Linee Guida Strategiche e della priorità degli interventi;
  – definizione di Standard Architetturali;
  – pianificazione e Controllo di Gestione;
  – controllo e *Audit* centrale;
  – pianificazione Operativa;
  – gestione operativa dei progetti;
  – gestione operativa dell'erogazione dei servizi;
  – controllo e *Audit* progettuale, con relativi *follow up* alle strutture centrali per la gestione delle iniziative sospese per termine dei finanziamenti o per altri impedimenti;

– una dimensione metodologica, che veda coinvolte alcune delle migliori pratiche metodologiche ai diversi livelli operativi, ad esempio:
  – *strategic alignment model* (Sam) per la definizione delle *linee guida* e della priorità degli interventi;
  – Cmmi[5] *for services* 1.2 per la definizione dei percorsi evolutivi e delle *road map* di intervento;

[5] *Capability maturity model for integration*, modello pubblico di fonte SEI/Carnegie Mellon finalizzato alla definizione dei modelli di progettazione, pianificazione strategica e operativa, misurazione e controllo di servizi secondo modelli incrementali di miglioramento successivo che tendono anche alla completa misurabilità dei processi di gestione non solo in termini di controllo ma soprattutto di efficientamento, secondo logiche industriali coerenti con i modelli stocastici Lean Six – Sigma, che rappresentano uno scenario naturale di evoluzione di questo approccio in un'ottica di Tom e riduzione della varianza della difettosità (restringimento della gaussiana di difettosità progettuale e di erogazione e orientamento ai «5 –9»).

  – Pmi[6] e/*o Prince 2*[7] per la gestione dei modelli di *Planning*;
  – modelli di analisi economico – finanziaria per la valutazione e il monitoraggio dei progetti in ottica Abc[8] secondo *driver standard* di Roi[9], *PayBack Period,* Irr[10], con modelli standard di controllo;
  – Itil[11] per la parte di *service Mangement*, quindi per l'impostazione, la progettazione, il dispiegamento, la transizione e la gestione operativa dei servizi;
  – Cobit[12] per quanto riguarda metodologie di controllo e di *audit*, sia strategico che operativo.

[6] *Project management institute*, ente indipendente titolare di una specifica metodologia di impostazione e gestione progettuale che include anche gli aspetti economico-finanziari.

[7] Metodologia di *Project management* di derivazione IBM, sovrapponibile alla precedente ma spesso indicata come naturale complemento ai modelli di *service management* Itil e di controllo Cobit.

[8] *Activity based cost*.

[9] *Return on Investment*.

[10] *Internal rate of return*.

[11] *It Infrastrcuture Library*, al momento alla versione 3.1, modello di gestione del *deployment* e dell'erogazione di servizi Ict nato in ambito Ufficio del commercio della Gran Bretagna e presidiato dall'*It Service Management Forum*. Il modello prevede l'intero processo di definizione delle esigenze, pianificazione strategica e operativa, progettazione, costruzione, *deployment* e *transitioning*, gestione operativa e misurazione di servizi It, sia singoli sia in logica di portafoglio (più servizi differenti o stesso servizio erogato con diverse caratteristiche, o in termini di attributi o in termini di Sl), identificando anche tutte le metriche e gli indicatori di controllo. Esso è riconducibile in parte al modello Cmmi attraverso apposite matrici di conversione che permettono di utilizzare in maniera integrata i due modelli.

[12] *Control Objective for It*, metodologia sviluppata nel mondo dell'*It Audit* da Isaca, *Information Systems Audit and Control Association*, associazione internazionale indipendente che definisce gli standard di Audit per i sistemi informativi e mantenuta e integrata dalla sua costola di ricerca. L'*It Governance Institute* (Itgi). Essa definisce le aree di processo, i Ksf, i Kgi e i Kpi per area di processo e sotto – processo per i la gestione di servizi e progetti Ict in una logica di misurazione e controllo e rappresenta lo strumento standard a livello mondiale per gli IS Auditor anche sul piano finanziario. Il Cobit è riconducibile in parte al modello Itil attraverso apposite matrici di conversione che permettono di utilizzare in maniera integrata i due modelli.

Tutti questi compiti di natura tecnica ed operativa si ripetono in ogni progetto di natura sistemica: nasce quindi l'esigenza sia di identificare un contenitore della cultura e delle competenze metodologiche di gestione progettuale, sia di un inquadramento, anche gerarchico, dei responsabili dei progetti. Come sempre si possono considerare più soluzioni, e alcune di ampio impatto, che prevedano, ad esempio, la costituzione di un'Agenzia con il compito di commissionare gli studi di fattibilità, di definire gli standard e di assicurare la realizzazione dei progetti nazionali a valenza sistemica della pubblica amministrazione: potrebbe essere articolata in funzioni architetturali per le linee guida, funzioni di *governance* e *risk management* e funzioni di *audit* e *compliance*, creando così un organismo operativo articolato e complesso di cui occorrerebbe individuare la opportuna collocazione istituzionale.

Il flusso di processo potrebbe essere, ad esempio, così articolato:

– il Dipartimento digitalizzazione e innovazione Pa identificherebbe le possibili iniziative progettuali, fornendo al livello strategico/politico (attualmente identificabile nella cabina di regia per l'agenda digitale) lo studio di fattibilità preliminare e i relativi elementi di valutazione;

– la cabina di regia opererebbe le opportune scelte, definendo la pianificazione strategica degli interventi e i relativi budget;

– il Dipartimento effettuerebbe le necessarie attività di predisposizione per gli articolati di legge richiesti e l'identificazione delle responsabilità organizzative;

– l'ipotizzata Agenzia sarebbe responsabile delle attività di impostazione progettuale in termini di studi di fattibilità, definizione delle specifiche tecniche e funzionali e predisposizione dei criteri di selezione, anche per eventuali gare, di cui seguirebbe l'aggiudicazione;

– l'aggiudicatario curerebbe le attività implementative e progettuali;

– l'Agenzia opererebbe il collaudo e sovraintenderebbe al rilascio;

– gli Enti partecipanti si occuperebbero dell'erogazione a regime del servizio;

– l'Agenzia si occuperebbe di effettuare le attività di *audit* e di *maintenance* rispetto alla continuità del servizio.

In figura il flusso sopra descritto:

Figura 14. Il flusso di processo

Il modello sopra rappresentato e i relativi supporti metodologici permettono un'applicazione operativa in diversi modelli organizzativi, dai più accentrati ai più distribuiti. L'unica tutela riguarda la gestione coordinata degli interventi in termini di:

– linee guida;
– priorità
– pianificazione strategica;
– controllo;
– architetture.

Tali attività possono anch'esse essere ricondotte a diversi scenari organizzativi e amministrativi, ma dovrebbero comunque garantire la capacità di una vista sistemica degli scenari evolutivi.

Resterebbero di responsabilità degli enti preposti alla gestione progettuale, collocabili a livello ministeriale per la pubblica ammi-

nistrazione centrale e a livello territoriale per la pubblica amministrazione locale, secondo i modelli di delega riconosciuti per legge e per prassi, tutti gli altri livelli:

– pianificazione operativa;

– *service management;*

– *audit & control* (con il supporto di associazioni professionali o di singoli professionisti accreditati).

Due gli esempi possibili:

– in un primo scenario le cinque attività sopra elencate vengono ricondotte alla responsabilità di un ente amministrativo unico, possibilmente indipendente dalle strutture settoriali, ministeriali o territoriali, assumendo natura di Agenzia autonoma o di struttura integrata posta sotto la responsabilità diretta della Presidenza del Consiglio: in tale veste la struttura sarebbe responsabile degli indirizzi, delle scelte strategiche e dell'erogazione e controllo dei finanziamenti alle strutture progettuali, distribuite amministrativamente e/o geograficamente, le quali manterrebbero piena autonomia per quanto riguarda sia la gestione operativa delle attività progettuali, sia per l'erogazione dei servizi, sia per la gestione dei fondi, stante però un quadro regolamentare definito a livello centrale. Di fatto, in questo scenario, l'Agenzia assumerebbe un ruolo comparabile a quello di Banca d'Italia rispetto al sistema bancario prima del Sistema monetario europeo, con in più un ruolo di tramite per la gestione dei finanziamenti e una forte focalizzazione sulle attività di vigilanza, allo scopo di evitare la nascita di cantieri privi di sbocco perché non adeguatamente finanziati o presidiati[13]. Portato di tale approccio sarebbe la nascita una struttura centrale molto articolata, con al proprio interno tutte le anime atte a garantire il ciclo di pianificazione e controllo, con la possibilità di operare anche interventi correttivi o integrativi in presenza di documentate lacune gestionali od operative sia in fase di dispiegamento sia in fase di rilascio. In questo modello sarebbe molto più facile sia individuare, e di conseguenza gestire, le componenti sistemiche di servizio sia definire modelli di business agibili anche da soggetti privati sui diversi ruoli, come definiti nel capitolo 1;

– in un secondo scenario il modello resterebbe simile, ma la struttura centrale perderebbe il controllo sui percorsi di finanziamento, che continuerebbero ad essere erogati direttamente agli enti preposti alla gestione progettuale senza intermediari, diventando di fatto solo una struttura di garanzia, con soli poteri di indirizzo e di controllo ma senza capacità di intervento operativo e senza il coordinamento con gli enti finanziatori. Questo scenario permetterebbe almeno il mantenimento di una prospettiva sistemica integrata, manterrebbe un elevato livello di responsabilizzazione dei singoli enti progettuali che avrebbe un riscontro operativo nelle strutture di controllo centrali[14]; questo scenario faciliterebbe la creazione di nodi di eccellenza distribuiti sul territorio, con un forte coinvolgimento pubblico e un deciso interesse anche da parte di *provider* locali, in funzione della capacità di pianificazione e controllo dei singoli enti progettuali, e richiederebbe la strutturazione di un modello di *controller* di linea esattamente sull'esempio dei modelli industriali più complessi, presentandosi l'ovvia difficoltà di monitorare gli investimenti e di rendere il modello di business sostenibile per operatori esclusivamente privati.

8. Le amministrazioni e la Nuvola pubblica certificata

Per contestualizzare il *cloud computing* nella pubblica amministrazione italiana è importante ricordare che la pubblica amministrazione dispone oggi di un'infrastruttura di connettività, il Sistema pubblico di connettività (Spc) disciplinato dal Capo VIII del Cad, con le modifiche ed integrazioni introdotte dal decreto legislativo 30 dicembre 2010, n. 235.

Si tratta di una rete di comunità privata, realizzata anche attraverso la federazione delle reti delle regioni, la cui principale finalità dovrebbe essere quella di consentire l'interazione diretta tra i *back end*

[13] Anche se si ritiene opportuno non affrontarlo in questi termini, questo è lo scenario di un «governatore dell'Ict» o Cio nazionale, con poteri di indirizzo e di gestione.

[14] Questo, invece, è lo scenario di un «Coordinatore nazionale» con forti capacità di indirizzo su una serie di Cio o capi-progetto Ict riferiti a specifici enti.

delle amministrazioni in modalità *business to business* (B2B), la cosiddetta «cooperazione applicativa», utilizzando i previsti servizi infrastrutturali di supporto (Spcoop). Spc fornisce inoltre i servizi di accesso ad internet per le amministrazioni connesse ed è quindi del tutto pertinente considerare i *provider* di Spc come Isp certificati e abilitati anche per la Nuvola pubblica certificata.

I servizi *cloud* sono tipicamente erogati da soggetti privati (in genere da soggetti dotati di grandi *data center*) e in base alla norme attuali del Cad[15] i *cloud provider* certificati, se soggetti privati, non sono compresi tra quelli ammessi ad erogare servizi direttamente su Spc**.** Tuttavia Spc fornisce alle amministrazioni anche il servizio di accesso a internet e pertanto, salvo eventuali problemi di banda, le amministrazioni sarebbero già oggi in grado di accedere ai servizi dei *cloud provider* se resi disponibili sulla Nuvola pubblica certificata.

Come già menzionato un'accelerazione in questo senso comporta la definizione di un *framework* di collaborazione pubblico-privato e l'attivazione di un progetto strategico di lungo periodo: il progetto dovrà garantire, da parte delle amministrazioni interessate, l'adozione pianificata dei servizi specifici richiesti ai *cloud provider* certificati e che tale adozione avvenga in tempi certi al fine di garantire ai *provider* il ritorno dell'investimento; il piano dovrà inoltre prevedere incentivi per le amministrazioni che favoriscano l'adozione di servizi *cloud*. Da ultimo va evidenziato che un simile piano richiede evidentemente un soggetto che lo governi e sia responsabile del raggiungimento degli obiettivi, analogamente a quanto segnalato nei precedenti paragrafi per ogni progetto nazionale a valenza sistemica.

Partendo dagli scenari sopra rappresentati quella che s'intende avanzare è una prima proposta, basata su alcune assunzioni, di cui si evidenziano le principali caratteristiche, i possibili benefici e i relativi impatti.

Lo scenario in cui ci si intende muovere è strumentale ad enfatizzare contemporaneamente la componente progettuale e quella di controllo. Rappresentano assunzioni del modello:

– la necessità di considerare l'Ict come infrastruttura critica con valore sistemico, tale da giustificarne una *governance* a livello nazionale;

– la conseguente necessità di effettuare una mappatura del valore sistemico dei servizi Ict o, comunque, della loro rilevanza per i servizi della pubblica amministrazione;

– il mantenimento dell'autonomia degli enti eroganti i finanziamenti, stante la necessità che la verifica e il controllo restino aggregati in una pianificazione strategica unica, almeno in termini di linee guida e di standard operativi e architetturali;

– la qualificazione di un modello di controllo che impedisca sia la proliferazione progettuale sia il loro abbandono o uso strumentale con relativa dispersione dei fondi.

Il modello si articola in due componenti:

– un'Agenzia di pianificazione strategica e di controllo;

– un consorzio operativo, basato sulle capacità infrastrutturali Ict di grandi operatori nazionali pubblici o privati con valore sistemico, esplicito o implicito che, mettendo a fattor comune la propria capacità, funzioni da elemento abilitante per i servizi ad alta priorità, contribuendo a sbloccare il mercato e a facilitare l'attivazione di un circuito virtuoso di *cloud providers*, magari più focalizzati sulle componenti di servizio a valore aggiunto che su quelle infrastrutturali.

[15] Art. 75 – *Partecipazione al Sistema pubblico di connettività*. 1. Al Spc partecipano tutte le amministrazioni di cui all'articolo 2, comma 2.

2. Il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n.165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale,consultazioni elettorali.

3. Ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 11 novembre 1994, n. 680, nonché dell'articolo 25 del decreto legislativo 30 giugno 2003, n. 196, è comunque garantita la connessione con il Spc dei sistemi informativi degli organismi competenti per l'esercizio delle funzioni di sicurezza e difesa nazionale, nel loro esclusivo interesse e secondo regole tecniche che assicurino riservatezza e sicurezza. È altresì garantita la possibilità di connessione al Spc delle autorità amministrative indipendenti.

3-*bis*. Il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al Spc e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all'articolo 79.

Capitolo Quarto

IMPATTI ORGANIZZATIVI E GESTIONE DEL CAMBIAMENTO

1. Premessa

Nel corso delle attività che hanno condotto alla realizzazione dello studio, alcuni temi sono ricorsi con una certa frequenza; questi sono stati: la riduzione dei costi conseguente l'adozione di soluzioni di *cloud computing*, la riduzione del personale, sempre indotto dall'adozione di soluzioni dello stesso tipo, gli impatti del federalismo sull'organizzazione della pubblica amministrazione locale e centrale e le conseguenti opportunità/problemi correlate all'adozione di soluzioni in *cloud computing* ed, infine, le complesse tematiche connesse con le logiche d'uso che le soluzioni in *cloud computing* comportano, cioè il tema che, con un termine solo, ma non per questo meno rilevante nell'articolazione dei contenuti, si è chiamata la *governance* del sistema.

All'ultimo punto, proprio per la sua rilevanza, è stato dedicato l'intero capitolo 3, ove si propongono anche degli interventi sul piano dell'architettura istituzionale che dovrebbe governare i complessi problemi di cui ci si occupa nello studio, per cui si rimanda a quel capitolo l'analisi dettagliata del tema e delle sue implicazioni. Sugli altri temi è probabilmente opportuno riprendere alcuni concetti già espressi, integrarli con altre considerazioni emerse durante i lavori dello studio e formulare delle valutazioni più sistematiche. Si inizierà quindi con il tema dei costi, successivamente si tratterà il tema delle risorse umane, che verrà visto non solo relativamente agli ambienti delle aziende/enti utenti ma anche di quelle dell'offerta, ed infine si affronterà il tema del federalismo o meglio delle sue relazioni con le caratteristiche che le soluzioni tecnologiche dovrebbero avere.

2. *Cloud computing* e costi

Si sono svolte in precedenza due «simulazioni», sul fascicolo sanitario elettronico e sul sistema informativo dei comuni, volti a fornire elementi di valutazione dell'effetto delle soluzioni in *cloud computing* sul tema dei costi; entrambi gli esercizi, seppur condotti in condizioni «sperimentali», cioè sviluppando dei modelli delle realtà che venivano considerate, hanno ampiamente dimostrato che la possibilità di ridurre significativamente i costi è reale, pur con tutte le necessarie cautele cui si è, per altro, accennato; tuttavia il tema non è stato esaurito, in quanto è stato trattato strettamente in relazione all'implementazione delle soluzioni e alla loro gestione e manutenzione, senza considerare la possibili riduzioni di costo «indotte» dall'utilizzo di simili soluzioni ma relative a voci di costo non di natura tecnologica: si vuole cioè dire che vi sono altri costi che le soluzioni in *cloud computing* riducono, liberando risorse economiche per altre attività e di ciò ci si occuperà in questo paragrafo.

Nel seguito l'analisi sarà condotta con riferimento più frequente al progetto del fascicolo sanitario, ma solo per un motivo strumentale, data la maggior disponibilità di riferimenti: le considerazioni che verranno svolte sono, comunque, assolutamente estendibili ai comuni e, in via più generale, a qualsiasi settore di mercato.

Con riferimento alla trattazione del fascicolo sanitario, nel caso dello «scenario evolutivo», quello cioè più conveniente in termini economici, si è assunta l'ipotesi d'implementazione di una piattaforma unica della soluzione in *cloud computing*; in questa ipotesi tutta una serie di costi verrebbero automaticamente a cessare dato che, ad esempio, le dotazioni locali di hardware per l'elaborazione dei dati, con le connesse spese per software, di assistenza, elettricità ecc., che oggi vengono utilizzate per gestire i vari servizi dell'area clinica che forniscono i dati per il Fse, non sarebbero più necessarie. Nel caso dei comuni si possono fare considerazioni simili, dato che anche in questo caso vi sarebbero riduzioni delle dotazioni di hardware con le relative conseguenze.

È evidente quindi che vi è la possibilità di valutare ulteriori riduzioni di spesa, al di là di quelle strettamente derivanti dalla sola implementazione dei progetti come delineati: vi sono infatti diverse altre voci su cui una soluzione *cloud based* porterebbe significativi risparmi, nell'ambito sia di minori costi per tecnologia sia di minori costi derivanti da un aumento del livello di efficienza dell'organizzazione nel suo complesso.

Con riferimento al secondo aspetto va detto che, purtroppo, non sono disponibili metriche che permettano di misurare *a priori* sul piano economico e trasformare l'aumento di efficienza in riduzione dei costi di gestione e pertanto non è possibile, per ora, effettuare delle valutazioni economiche di questo aspetto, che abbiano almeno un minimo di aderenza alla nuova realtà che si verrebbe a delineare. Per quanto riguarda il primo, alcuni approfondimenti si possono fare, e precisamente:

– riduzione delle dotazioni hardware (*server*) (con riferimento alle Asr quelli per la gestione delle aree cliniche, incluse quelle diagnostiche; per i comuni, soprattutto quelli di minori dimensioni, quelli per la gestione dell'attuale «sistema informativo») con conseguente riduzione delle spese di gestione operativa e di manutenzione (questo documento, con riferimento alle Asr, non tratta le aree amministrativo-contabili in quanto non producono informazioni per il fascicolo sanitario, ma è evidente che anche a queste potrebbe essere applicato un modello analogo e quindi essere fornite in modalità *cloud computing*; in questa ottica le dotazioni hardware potrebbero essere ulteriormente ridotte, con conseguente riduzione dei costi di tutte le voci correlate);

– riduzione delle spese di manutenzione e di manutenzione correttiva ed adeguativa dovuta a cambiamenti normativi, in quanto queste attività potrebbero essere fatte un'unica volta, contrariamente alla situazione attuale che impone la ripetizione di queste operazioni (e dei relativi costi) per tutte le installazioni, non essendo possibile alcuna forma di economia di scala;

– riduzione delle spese di adeguamento tecnologico hardware e software: nel caso dell'adozione della piattaforma unica, indipendentemente al numero di «punti» di erogazione del servizio applicativo, questo intervento verrebbe fatto «una volta sola» e manterrebbe evidentemente «allineato» tutto l'ambiente, con l'eliminazione dei costi derivanti dal disallineamento tecnologico, inevitabile nella situazione attuale; per di più non esiste nessun piano generale per l'evoluzione tecnologica delle Asr o dei comuni e quindi ogni

ente opera come meglio crede, con conseguenti duplicazioni di interventi e spreco di risorse;

– riduzione delle spese per le piattaforme di sistema (sistemi operativi, data base, *application server*, ecc.) in quanto sarebbe possibile fare un contratto a livello nazionale e quindi acquisire i prodotti e la loro manutenzione a prezzi più vantaggiosi. Nella situazione attuale non si conosce neppure la spesa delle Asr e dei comuni per questi software, e neppure i differenti impegni contrattuali stipulati con i fornitori;

– riduzione della spesa legata all'adozione di standard dei dati, fatto strettamente connesso all'adozione di una piattaforma unica: oggi ogni Asr, e nei comuni la situazione non è molto dissimile, «parla» un suo «dialetto» per quanto riguarda i dati, che sono codificati e descritti con semantiche «locali»; ciò si riflette naturalmente sulle applicazioni e sulla loro possibilità di integrazione e di reciproca comunicazione: l'adozione di standard dei dati su un'unica piattaforma applicativa – sono eventualmente disponibili anche classificazioni internazionali – eliminerebbe tutti i costi connessi ai problemi precedentemente esposti. È evidente che il tema della standardizzazione dei dati e della loro semantica oggi rappresenta uno degli ostacoli per la realizzazione del fascicolo e di una soluzione per i comuni come quelle descritte;

– riduzione, se non completa eliminazione, della spesa per l'integrazione tra gli applicativi software, oggi altro grosso ostacolo alla realizzazione del fascicolo; si aggiunga, a questo, la necessità crescente per le Asr di integrare i processi clinico-sanitari tramite l'integrazione dei software che li gestiscono (ad esempio i percorsi diagnostici terapeutici assistenziali) in una visione integrata dell'approccio al malato; altro aspetto legato a questo tema è la necessità di creare strumenti per il controllo della spesa tramite anche l'interfacciamento dei software della parte clinica (oggi molteplici, disomogenei ed incompatibili) e quello dell'area amministrativo-contabile.

I punti sopraelencati, per lo meno quelli con valenza esclusivamente tecnologica, si possono dettagliare al fine di determinare un valore economico:

– l'eliminazione dei *server* comporta l'eliminazione dei canoni per le infrastrutture e gli ammortamenti relativi, i canoni per l'assistenza, in certi casi h24, quelli per il software di base e le spese per il personale esterno che svolge supporto in loco;

– la riduzione della manutenzione correttiva ed adeguativa si traduce nell'eliminazione dei canoni riconosciuti ai fornitori per le nuove versioni e le patch e delle spese per il personale esterno che installa il software;

– le spese per il mancato adeguamento tecnologico[1] che rappresentano, secondo fonti internazionali, una percentuale compresa tra il 10 ed il 15 % del valore dell'hardware e del software installato e che, anche se non viene effettuato durante la vita delle dotazioni hardware e software, genera comunque un sovra-costo al momento del cambio delle apparecchiature; in ogni caso genera un extracosto sotto forma di diminuzione dell'efficienza dei sistemi durante gli anni in cui l'adeguamento non è stato effettuato.

Alla luce di queste considerazioni si sono rilevati i costi sostenuti per le attività di cui sopra presso Asr di dimensioni differenti: si sono ottenuti valori ovviamente variabili, in funzione sia della dimensione delle Asr, sia del livello di sviluppo delle soluzioni; si è quindi optato per determinare due valori, massimo e minimo, come stime della possibile ulteriore riduzione dei costi, considerando quindi non più solo la pura fase di implementazione: tali valori di riduzione sono risultati pari a 220 milioni di euro come valore minimo e a 270 milioni di euro come valore massimo. Si è di fronte certamente a un valore considerevole ma, alla luce delle considerazioni fatte in precedenza sugli orientamenti della spesa Ict della Asr e sulla sua dimensione, si possono ritenere congruenti con tali valori. Considerazioni analoghe portano a stimare tale valore per i comuni in un intervallo compreso tra i 180 e i 220 milioni di euro.

Occorre tuttavia considerare che, a fronte di questi possibili risparmi, vi sarebbero costi aggiuntivi dovuti al processo di sostituzione dei sistemi applicativi e, per certi versi, della filosofia generale

[1] Aspetto questo trascurato, tenuto conto della numerosità e eterogeneità delle applicazioni software e delle tecnologie sottostanti di cui le Asr nel tempo si sono dotate.

delle nuove soluzioni; questi costi sono riconducibili ad attività di sensibilizzazione degli operatori sanitari e comunali, agli impatti organizzativi conseguenti, piuttosto che all'ostilità degli stessi operatori che potrebbe rendere il processo di cambiamento ancora più complesso; è inoltre evidente che progetti di queste dimensioni richiedono di essere realizzati per fasi, secondo un piano inevitabilmente pluriennale, con conseguente distribuzione dei costi d'implementazione su più anni e di un diverso andamento dei costi di gestione e manutenzione: i risparmi, che sopra sono definiti come complessivi, sarebbero certamente distribuiti nel tempo. Qui tuttavia non si è voluto scrivere un *business plan* ma, come detto, esplicitare le possibilità di riduzione dei costi al fine di fornire elementi di valutazione tra differenti possibili soluzioni.

Tre ultime considerazioni vanno fatte, e di grande importanza, che permettono di delineare un quadro generale, e che verranno riprese anche successivamente:

– la scelta dell'adozione di progetti analoghi a quelli descritti richiede la necessità di una «guida» unica in grado di definire e implementare la strategia necessaria, definire gli standard, definire le varie componenti del progetto, coordinarne e finanziarne la realizzazione; in altre parole vi è la necessità di costituire una struttura a livello nazionale (struttura di *governance*) che abbia il mandato di definire e realizzare (o fare realizzare, ma sempre sotto le proprie direttive) gli aspetti sopra indicati e che abbia il compito di mettere in atto tutte le azioni necessarie presso le Asr o i comuni, di cui si detto nel capitolo precedente;

– soluzioni come quelle descritte implicano una riduzione del personale direttamente addetto alla gestione dei sistemi informativi di cui, comunque, si tratterà più ampiamente nel seguito; va però osservato che nuove esigenze si pongono: un progetto di queste caratteristiche comporta un forte mutamento nei processi e nelle regole della *governance* di tutto il sistema, sia nei *modus operandi* degli addetti sanitari o comunali, a qualunque categoria essi appartengano; il progetto infatti porrebbe gli enti e gli operatori di fronte a scelte, relative ai processi come sarebbero svolti e alle tecnologie per supportali, senza che gli operatori stessi abbiano le necessarie conoscenze per valutarne gli affetti e le conseguenze; vi è quindi la necessità di guidare e governare il processo di mutamento, organizzandosi per superare l'inevitabile inerzia ed opposizione da parte delle strutture e degli operatori, atteggiamenti che potrebbero addirittura portare al fallimento dell'iniziativa: lo sviluppo del progetto va quindi accompagnato da una forte azione di informazione e di formazione, di promozione e di supporto verso le strutture e gli operatori in una sorta di processo di *governance* condivisa, in modo da renderli partecipi delle finalità del progetto stesso. In questa attività, di fondamentale importanza per la buona riuscita del progetto, potrebbe trovare occupazione il personale che si rendesse disponibile, svolgendo le necessarie attività di supporto per l'avvio e la gestione delle attività;

– il progetto descritto contiene una forte carica innovativa, destinata a modificare abitudini e mentalità, senza che sia sempre possibile per i singoli operatori comprenderne immediatamente i vantaggi, in quanto spesso di ordine «generale», relativi al Paese più che alla singola struttura in cui gli operatori operano: ciò richiede pertanto strumenti adeguati per l'implementazione. Lo schema generale, che emerge delle precedenti considerazioni, utile per affrontare la complessità delle attività da svolgere, può essere quello di un sistema di *governance* «a più livelli», con una forte componente di condivisione interna al sistema stesso: una struttura nazionale con i compiti sopra delineati, che dispiega la propria azione tramite le regioni, con il supporto dei tecnici e degli specialisti resi disponibili presso i sistemi informativi.

Sempre con riferimento alla possibilità di riduzione della spesa si possono fare ulteriori simulazioni facendo però delle stime a carattere più indicativo, sempre per fornire elementi di valutazione. Senza scendere nel dettaglio si considerino ad esempio le regioni: da un punto di vista tecnologico nulla osta a che si possa adottare un'unica soluzione in *cloud computing* valida per tutte le regioni e resa loro disponibile da un unico punto di erogazione: i vantaggi sarebbero evidenti in termini d'integrazione delle informazioni, in campi ben definiti e delimitati, e della conseguente maggior incisività che l'azione di governo potrebbe avere, ad esempio per la gestione del territorio piuttosto che per la lotta all'inquinamento, proprio a livel-

lo regionale; una soluzione di questo tipo potrebbe automatizzare, con le medesime applicazioni, probabilmente la maggior parte delle attività svolte dalle regioni, lasciandone una componente minore a soluzioni specifiche e «proprietarie» delle singole regioni. È evidente che, in una simile prospettiva, verrebbero implementate tutte le garanzie di sicurezza e riservatezza dei dati, assicurando la completa autonomia e responsabilità delle regioni: d'altro canto un'ampia gamma di attività regionali sono «uguali» tra loro, basti pensare alle attività amministrative! Le conseguenze in termini di riduzione dei costi sarebbero significative: probabilmente intorno ai 240 milioni di euro l'anno, a fronte di una spesa attuale pari al più del doppio; per una valutazione precisa occorrerebbe fare un esercizio simile a quelli svolti per il fascicolo sanitario elettronico e per i comuni, ma in questa sede si vuole solo indicare ulteriori possibili aree di riduzioni dei costi. Considerazioni simili si possono fare per le province, sempre che non vengano eliminate: oggi si stima spendano circa 80 milioni di euro l'anno, nel caso di soluzione in *cloud computing* la spesa sarebbe probabilmente ridotta a 25-30 milioni di euro l'anno.

Si può pertanto ragionevolmente ritenere che a fronte di una spesa annua degli enti locali (regioni, comuni e province) attualmente di poco superiore a 1,1 miliardo di euro, secondo i dati ricavabili da quanto pubblicato dalle principali società di ricerche di mercato, la diffusione, negli stessi enti, di soluzioni in *cloud computing* permetterebbe una riduzione dei costi stimabile in circa 640 milioni di euro l'anno, con riferimento ai costi di esercizio. Naturalmente occorrerebbe definire, per regioni e province, modelli di soluzioni in *cloud computing* analoghi a quanto fatto per i comuni e per il fascicolo sanitario e calcolare i relativi costi d'implementazione, per avere un quadro completo, cosa che tuttavia esula dagli obiettivi del presente studio: pur con questa limitazione, è inequivocabile che i costi di gestione sarebbero significativamente minori, senza contare i molteplici vantaggi sul piano organizzativo e funzionale, cui si è già detto a proposito dei comuni e del fascicolo sanitario

È tuttavia opportuno, a questo punto dell'analisi, chiarire alcuni aspetti: si è visto che riduzioni dei costi sono possibili per quanto riguarda la spesa It, ma anche che non sono ad oggi disponibili metriche generali che permettono di inferire conclusioni generali a

priori sul fronte delle possibili riduzioni di costi da maggior efficienza delle organizzazioni: occorre, per valutare questi aspetti, fare dei precisi studi di fattibilità che tengano conto di tutte le variabili in gioco. Da questo punto di vista si è più volte ricordato che, in questa sede, si sono fatti degli esercizi di simulazione, comunque con risultati d'indubbio interesse, seppur con riferimento alle sole componenti tecnologiche. La mancanza di metriche generali valide per la misurazione degli effetti delle soluzioni in *cloud computing* anche sugli aspetti organizzativi e dell'aumento dell'efficienza, non può tuttavia diventare una sorta di alibi per non metter mano a progetti come quelli descritti: il paese non può aspettare ulteriormente che vengano fatte analisi e tratte conclusioni «generali», cui si è per altro già pervenuti, seppur in modo parziale e per «campioni»; come anche non sono più procrastinabili veri e profondi interventi volti a rompere determinate prassi e a introdurre concrete iniziative innovative basate, oltre che su una diversa visione pubbliche amministrazioni, anche sull'utilizzo dei nuovi strumenti tecnologici. Certo gli ostacoli da affrontare sono molti, non ultimi le possibili resistenze di alcuni fornitori o di alcune categorie di lavoratori (una soluzione come quella delineata per i comuni incontrerebbe sicuramente l'opposizione degli addetti a particolari settori quali ad esempio quelli dell'edilizia privata); un altro ostacolo è l'autonomia degli enti locali, spesso intesa come una sorta di completa «discrezionalità decisionale», tema sul quale occorre lavorare, secondo il dettato costituzionale, nella direzione della sussidiarietà: ciò che pare oggi particolarmente importante e urgente è la possibilità di sfruttare le opportunità che la tecnologia mette a disposizione, avendo tuttavia la capacità di implementare e rendere operative le necessarie strutture funzionali con gli adeguati compiti e poteri decisionali, in grado anche d'intervenire sulle attività degli enti.

3. *Cloud computing* e risorse umane

Il tema della relazione tra utilizzo di soluzioni in *cloud computing* e risorse umane è solitamente discusso con riferimento, quasi esclusivo, al personale dell'azienda o organizzazione utente di tali soluzioni. In verità il tema ha una valenza più ampia in quanto, se è vero

che riguarda la struttura utilizzatrice, è altrettanto vero che è destinato ad avere impatti anche sul fonte dell'offerta e delle relazioni tra operatori dell'offerta e della domanda, ciò indipendentemente dallo specifico segmento di mercato.

Si considerino per primi gli effetti della «logica» *cloud computing* sulle relazioni tra domanda e offerta, tra cliente e fornitore. Le osservazioni che seguono potrebbero essere considerate troppo generali e più pertinenti al caso di organizzazioni private di dimensioni medie e grandi; sono considerazioni di «mercato» e sono comunque applicabili a qualunque segmento, anche agli enti della pubblica amministrazione centrale o locale: la loro generalità deve, al contrario, fornire elementi di valutazione per «caratterizzare» i fenomeni attesi allo specifico settore pubblico.

La diffusione di servizi proposti in *cloud computing*, proprio per le caratteristiche proprie di questa modalità di erogazione, potrà comportare l'introduzione di alcune componenti innovative nel processo di acquisto, valutazione della «fornitura» e, più in generale, di gestione del rapporto tra cliente e fornitore:

– date le caratteristiche dei servizi *cloud*, l'interlocutore del fornitore di soluzioni Ict può divenire l'utente finale, la funzione dell'organizzazione che è l'utilizzatrice della soluzione, che non ha competenze tecnologiche specifiche ma elevate competenze sul processo aziendale interessato dall'utilizzo dello specifico servizio; si pongono due problemi: da un lato la difficoltà dell'utente a valutare gli aspetti tecnologici, non essendo «esperto» di tecnologia, dall'altro la necessità per il fornitore di conoscere approfonditamente i processi di cui offre la soluzione; un simile fenomeno, di sostanziale disallineamento, potrà comportare una significativa modifica nelle relazioni tra fornitore e cliente, con impatti sull'intero processo di gestione della domanda; evidenzia tuttavia la necessità di nuove figure professionali o per lo meno di modifica di alcune delle professionalità attuali;

– per quanto riguarda la valutazione della fornitura, va considerata una nuova potenziale difficoltà: l'utente, come detto, non ha competenze tecnologiche ma dei processi aziendali pertanto, a fronte di Sla e clausole contrattuali che definiscono i livelli di servizio, non dispone degli stessi strumenti di valutazione utilizzati dal fornitore (e della struttura It dell'azienda/ente utente) correndo il rischio di effettuare valutazioni con una significativa componente di soggettività; potrebbe nascere quindi una possibile «divergenza» nelle attività di monitoraggio e valutazione, con prevedibili riflessi sul piano della gestione contrattuale: anche in questo caso è prevedibile la necessità di opportune figure professionali che intervengano a gestire gli eventuali conflitti.

Le considerazioni fatte hanno evidentemente riferimento prevalentemente al caso di servizi SaaS, che hanno una valenza applicativa tale per cui l'interlocutore può essere la funzione dell'organizzazione proprietaria del processo; differente è il caso di servizi IaaS e PaaS che, per il loro elevato contenuto tecnologico è prevedibile restino di competenza della struttura tecnica del cliente. In ogni caso, tuttavia, una soluzione *cloud based* impatterà inevitabilmente sui processi dell'organizzazione e necessiterà comunque di essere inquadrata in una vista «unificante» che è appunto quella della struttura It; questa, tendenzialmente, prenderà in carico la gestione di tutti i servizi acquisiti in *cloud* e il suo coinvolgimento sarà funzione della complessità tecnologica dei servizi stessi: per i servizi *cloud* a prevalente contenuto tecnologico (IaaS, PaaS) il coinvolgimento sarà maggiore se non completo, mentre per i servizi maggiormente legati agli aspetti di processo dell'utente (SaaS) tale coinvolgimento sarà inferiore e si espliciterà in una funzione di supporto «consulenziale» nella definizione degli Sla, nelle attività di monitoraggio della fornitura ed in eventuali attività successive di integrazione applicativa.

La discussione condotta, come si è detto, è relativa prevalentemente ad utenti medi e grandi di qualunque segmento di mercato: mostra però la necessità di figure professionali relativamente nuove; problemi e prospettive analoghe si aprono, tuttavia, anche per gli utenti minori, più probabili destinatari di soluzioni basate su *cloud pubblico*, quali appunto molti tra gli enti pubblici locali; non vi sono motivi per ritenere che simili utenti possano utilizzare servizi *cloud* con un livello di complessità inferiore, ma vi è un livello di «complessità» minore nell'utente e quindi una possibile maggior difficoltà nel gestire i rapporti con i fornitori e valutare i servizi ricevuti:

non è improbabile, in questa prospettiva, la nascita di nuovi operatori (o la trasformazione di alcuni degli attuali) con competenze di tipo consulenziale, che possano sopperire alle carenze degli utenti, sia nell'individuazione delle soluzioni più efficaci sia nell'attività di controllo della fornitura dei servizi.

Sin qui si è visto che determinati fenomeni attesi avranno prevalentemente conseguenze sul piano della modifica delle professionalità più che su quello della riduzione del personale, ciò grazie alla necessità, sia per il cliente sia per il fornitore, di gestire nuovi problemi e nuove possibili criticità.

Per quanto riguarda più strettamente il tema della riduzione del personale, con particolare riferimento a soluzioni di *cloud pubblico*, si può prevedere che:

– la riduzione è prevedibile possa essere «allineata» alle aree di riduzione dei costi: manutenzione hardware, sviluppo e manutenzione adeguativa delle applicazioni, attività frequentemente svolte da personale esterno, essendo abitualmente il personale interno riservato a quelle a maggior valore aggiunto;

– per quanto riguarda dove e in che misura si verificherebbe la prevista riduzione del personale, sempre con riferimento a soluzioni di *cloud pubblico* si può osservare che nei «punti» di erogazione dei servizi tale riduzione sarà inevitabilmente ridotta, in quanto vi permarrà comunque un grande volume di attività con, in più, la necessità di supporto tecnologico e consulenziale presso le organizzazioni utenti per la gestione delle nuove modalità di erogazione delle applicazioni;

– negli utilizzatori di minori dimensioni, serviti dai «punti» di erogazione dei servizi *cloud*, la riduzione del personale potrebbe essere maggiore: tuttavia occorre considerare due aspetti: questi utenti, che comunque già oggi dispongono di limitate strutture dedicate alla gestione delle tecnologie, da un lato avranno in ogni caso necessità di un presidio tecnologico, anche se ridotto, dall'altro avranno necessità di forme di supporto consulenziale di cui oggi non hanno necessità.

Alla luce di queste considerazioni si può ritenere che il tema che emerge è soprattutto la necessità di disporre di personale con nuovi profili professionali, quindi di riqualificare quelli che in prima approssimazione diverrebbero superflui:

– presso gli utenti di maggiori dimensioni, con soluzioni in *cloud privato* o *ibrido*, serviranno nuove professionalità per la gestione delle tecniche di *Services management*, in quanto la struttura It muta di ruolo, per la attività di modellazione e previsione della domanda di servizi, per la valutazione delle forniture e del loro adeguamento alle clausole contrattuali, per il supporto all'espansione dell'uso della tecnologia nell'organizzazione, sicura conseguenza del basso costo dei servizi *cloud*;

– per gli utenti di dimensioni minori, con soluzioni in *cloud pubblico*, oltre comunque al personale necessario alla gestione delle dotazioni tecnologiche che, seppur in misura ridotta, resteranno installate, servirà personale con capacità consulenziale per la gestione del cambiamento di paradigma, ed inoltre per gestire, come indicato anche per gli utenti di maggiori dimensioni, il prevedibile aumento dell'intensità d'uso della tecnologia Ict, mediante l'adozione di un maggior numero di applicazioni, disponibili a basso costo.

Queste nuove professionalità potranno venire dalla riqualificazione del personale sia interno sia esterno: in questo caso, inoltre, potranno dare vita anche a nuove iniziative imprenditoriali nell'area della consulenza. A questo proposito è utile fare qualche ulteriore osservazione con riferimento al mondo dell'offerta, pur se vanno svolte considerazioni differenti per gli operatori di grandi dimensioni e i minori e piccoli: per i primi la struttura del business si modificherà nella direzioni di un contributo inferiore da licenze software e da hardware ma con aumento della componente servizi (IaaS, PaaS, SaaS) e di quella legata alle attività di consulenza, che si sposteranno dall'ambito strettamente It alle tematiche più vicine all'operatività dell'utente; per i secondi è probabile, da una parte, un'accelerazione del processo di razionalizzazione della struttura del comparto industriale Ict tramite acquisizioni e fusioni di aziende, processo per altro già in corso e, forse, anche in parte necessario per migliorarne la «qualità» e la capacità di «stare sul mercato» e, dall'altra, lo svi-

luppo di nuovi *business model* «misti», composti da sviluppo di propri software, da *royalty* da *cloud provider* cui sia stato ceduto proprio software e da attività di servizi verso gli utenti delle proprie soluzioni fornite in *cloud*. Va comunque considerato che, sul fronte dell'offerta, emergeranno attori che oggi non hanno, o hanno in misura limitata, un'offerta applicativa, come gli operatori di telecomunicazione o gli *hosting provider*: questi operatori dispongono di un'offerta infrastrutturale che può essere completata con un'offerta applicativa, ad esempio tramite accordi con terze parti che abbiano sviluppato proprie soluzioni compatibili col *cloud*; va inoltre sottolineato che, in generale, questi nuovi operatori non dispongono già di un'offerta di tipo consulenziale, soprattutto nell'area dell'operatività aziendale, ma che comunque dovranno organizzarsi per disporre in proprio, o tramite accordi con operatori specializzati, di un'offerta adeguata in questa area. In un contesto in evoluzione è inoltre ipotizzabile la nascita di *cloud provider* altamente specializzati, con offerte verticali non inerenti il *core business* delle aziende e degli enti utenti, ma servizi orizzontali generali: per questo tipo di fornitori sono ipotizzabili forme di «regolamentazione» e di «certificazione» anche per servizi rivolti al mondo privato.

Il tema del personale resta, comunque, critico: non si è voluto descrivere uno scenario forzatamente ottimistico per evitare di affrontare le criticità che il problema pone: si è solo voluto presentare uno scenario possibile, articolato in tutti i suoi aspetti, rispetto al quale non ci sono fattori ostativi dovuti alla diffusione delle soluzioni in *cloud computing*; certo devono verificarsi alcune condizioni «al contorno» che, tuttavia, riguardano le caratteristiche e la struttura del settore delle tecnologie Ict in Italia e, probabilmente, sarà utile anche un differente atteggiamento di forze politiche e amministratori verso l'innovazione: il *cloud computing* è un fattore di profondo mutamento nella direzione della diffusione dell'innovazione, è certamente un fattore di forte discontinuità ma il tema della riduzione del personale che indurrebbe non deve divenire, anche in questa caso, un alibi per rinviarne l'utilizzo e la diffusione.

4. *Cloud computing* e federalismo

Più volte, nel corso dei lavori dell'Osservatorio, è emerso il tema del federalismo o, meglio, si è accennato al fatto se il federalismo possa influenzare le architetture applicative delle soluzioni tecnologiche quali quelle in *cloud* o, al contrario, se la diffusione delle soluzioni in *cloud computing* passa essere un fattore di supporto all'implementazione del processo federalista e, anche in sede di definizione dello schema dello studio, si è posto proprio il federalismo come fattore critico da considerare nello scenario generale per i possibili effetti sulla pubblica amministrazione e, conseguentemente, sulle strategia di implementazione delle soluzioni in *cloud computing*.

Prima di svolgere alcune considerazioni sul federalismo e sullo stato del suo processo di sviluppo, è utile fare alcune osservazioni sulla situazione attuale:

– l'architettura istituzionale del Paese è decisamente articolata e prevede un numero di livelli istituzionali e burocratici decisamente significativo;

– il sistema degli enti territoriali è, conseguentemente, in parte farraginoso è ciò rende le relazioni del cittadino con tale sistema complesse, a volte poco trasparenti e fonte di perdite di tempo;

– l'ottica degli apparati burocratici è di considerare il cittadino un proprio «ambito» di operatività, costringendolo a sostituirsi a loro nelle attività a «minor valore aggiunto», per tutte quella di trasportatore di documenti («camminatore» era termine presente nelle piante organiche degli enti pubblici centrali ed indicava la persona addetta al trasporto fisico delle pratiche, ma all'interno dell'ente);

– la diffusione delle tecnologie Ict si è sviluppata, come osservato in precedenti punti dello studio, in modo frammentato, privilegiando la visione localistica e senza alcuna visioni sistemica e nazionale.

A fronte di queste considerazioni, altre possono essere fatte a proposito del federalismo:

– il processo è di fatto fermo, ormai da 10 anni, da dopo l'approvazione del nuovo Titolo V della Costituzione;

– in ogni caso non vi è traccia di una riforma degli enti territoriali, della loro distribuzione e dei loro compiti, nella direzione della specializzazione, della semplificazione e razionalizzazione dei pro-

cessi e delle relazioni tra gli enti e tra questi e i cittadini;

– quanto previsto dallo stesso Titolo V in termini di architettura istituzionale si è trasformato nel complicarsi degli aspetti istituzionali e amministrativi, anziché esprimere la forte carica riformatrice che era prevista;

– non sembra esserci la percezione della necessità di ridisegnare l'architettura istituzionale contemporaneamente al ridisegno delle funzioni attribuite agli enti locali, riavvicinando l'amministrazione alle necessità dei cittadini.

Non si può comunque ritenere abbandonato il tema del federalismo, in quanto processo necessario per accompagnare il paese sulla strada della ripresa e dello sviluppo: è quindi un fatto con cui inevitabilmente anche le soluzioni tecnologiche dovranno fare i conti.

In questa prospettiva si possono valutare i seguenti aspetti:

– il federalismo comporterà inevitabilmente il trasferimento di funzioni tra livelli diversi della struttura istituzionale, ma ciò non potrà determinare una diversità di trattamento verso cittadini e imprese variabile nelle diverse aree territoriali: in altre parole dovranno comunque essere garantiti i medesimi servizi con la medesima qualità in qualunque area del territorio: a fronte dell'aumento dell'autonomia degli enti, la standardizzazione delle strutture dei dati, della loro semantica e degli aspetti applicativi e l'accessibilità da qualunque luogo che sono caratteristiche delle soluzioni in *cloud computing* sono la risposta più efficiente ed efficace ai problemi prima indicati.

– vale la pena ribadire quanto appena detto a proposito di un aspetto particolarmente critico: cittadini e imprese possono avere necessità di usufruire di determinati servizi da luoghi diversi da quelli di abituale residenza, aspetto che oggi è spesso fonte di disservizi anche gravi. Il federalismo deve favorire la standardizzazione dei servizi e delle modalità della loro erogazione verso cittadini e imprese da qualunque punto del territorio, possibilità resa concreta proprio dalle soluzioni in *cloud computing*;

– il risultato del federalismo deve favorire la comunicazione tra i sistemi di *back end* della amministrazioni, non la loro chiusura, aspetto anche questo reso concreto dell'utilizzo di architetture in *cloud computing*, grazie alla vocazione alla standardizzazione dei dati e delle applicazioni che lo caratterizza.

Il federalismo, oltre a comportare una diversa distribuzione delle funzioni tra gli enti, aspetto che si tradurrà in un ridisegno delle applicazioni e che potrebbe trarre grande vantaggio proprio dalle logiche di *cloud computing*, implica la necessità di definire un'infrastruttura Ict che abbia valenza strategica nazionale: ciò si impone assolutamente non solo in relazione all'evoluzione in senso federale dello Stato, ma anche nella prospettiva di razionalizzare e consolidare i sistemi informativi della pubblica amministrazione, per ottenere i benefici economici derivanti dallo stare al passo dell'evoluzione tecnologica e per garantire la sicurezza strategica del Paese e la sua capacità competitiva.

Vi è un ultimo importante aspetto da sottolineare, peraltro già indicato nel capitolo 3, la necessità e le caratteristiche della struttura di *governance*: l'evoluzione della architettura istituzionale verso il federalismo, ed il conseguente decentramento amministrativo, richiederanno iniziative di *governance* mirate da un lato a garantire l'interoperabilità dei processi, dei dati e dei servizi tra i livelli centrale, regionale e locale della pubblica amministrazione, dall'altro la necessità di mettere a disposizione soluzioni condivise; questo per evitare che l'autonomia delle regioni e degli enti locali, nella realizzazione di servizi, comporti lo sviluppo di soluzioni funzionalmente e tecnologicamente diverse come risposta a identici requisiti funzionali: in questo modo le soluzioni adottate potrebbero risultare non omogenee e non interoperabili tra loro, con conseguenze difficoltà di gestione, drastica riduzione della loro efficacia e aumento della spesa nel suo complesso: a questi problemi è essenziale faccia fronte una adeguata struttura di *governance*.

APPENDICI

APPENDICE 1

IL MODELLO ARCHITETTURALE

Chiaramente non è obiettivo di questo lavoro disegnare *in toto* o in parte ipotesi di sistemi informativi o di architetture tecnologiche di dettaglio.

Appare invece importante riferirsi a modelli architetturali standard, come quello del Nist per qualificare le opportunità offerte dai modelli *cloud* per abilitare con maggiore facilità l'erogazione dei servizi e la standardizzazione dei processi a supporto, da quelli di base, relativi alla sicurezza, all'alta affidabilità e al *recovery*, fino ai processi di *business* veri e propri.

Punto di forza, in particolare, è rappresentato da:

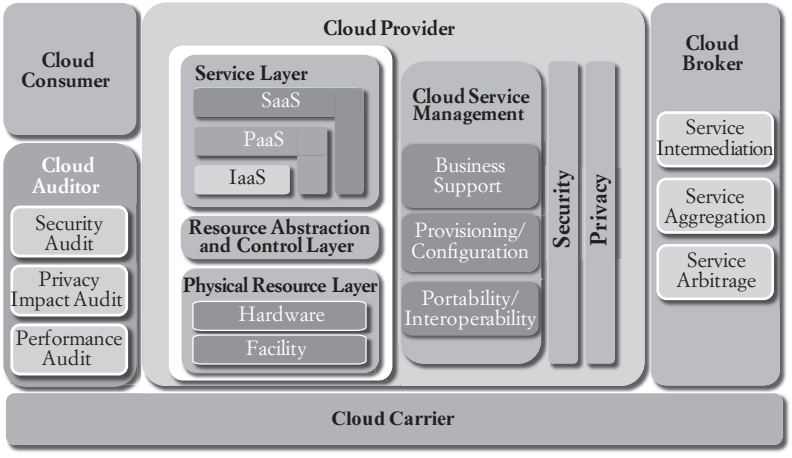
– la connotazione nativa nella stessa architettura *cloud* relativa all'alta affidabilità del servizio e alla sua capacità di *recovery* in ottica di servizio;

– il completo disaccoppiamento funzionale e tecnologico dei diversi *layer* che permette di sviluppare in maniera indipendente le diverse funzionalità senza legami tecnologici o di standard e di interagire con servizi già esistenti senza richiedere complesse attività d'integrazione;

– la possibilità di focalizzare quindi l'attenzione sullo sviluppo dei servizi applicativi e di processo più specifici per l'erogazione del servizio finale senza dover curare l'intera filiera tecnologica.

In sintesi il modello sotto descritto permette, dato un riferimento *cloud* di base, anche solo infrastrutturale, di sviluppare il modello servizi a *layer* successivi completamente indipendenti sia tecnologicamente sia in termini di *provisioning*.

Figura 15. Il Framework NIST



Il modello architetturale permette quindi, una volta abilitata una soluzione *cloud*, di effettuare tutti i livelli di integrazione indipendentemente dal punto di partenza, che esso sia il servizio finale o i servizi infrastrutturali di base o abilitanti di *security* o *recovery*, limitando il tema dell'integrazione ad un tema di interazione tra servizi, stante chiaramente la possibilità di accesso di rete.

La struttura a *layer*, che nella sua rappresentazione grafica sembra riprendere modelli tradizionali di architetture applicative *multitier*, in realtà qualifica una vera architettura di *provisioning* basata su pure logiche funzionali e non tecnologiche.

Ciò significa che è possibile immaginare sia uno scenario in cui fornitori specializzati forniscano una soluzione orientata all'erogazione del servizio finale, appoggiandosi su *layers* sottostanti erogati anche in maniera *on premise* sia che il servizio venga erogato in maniera *on premise* appoggiandosi per infrastruttura, servizi di *middleware* e di sviluppo o di *security* su soluzioni *cloud,* sia la costruzione di soluzioni *cloud* che si appoggino ad una sorta di «modello *cloud* unico», e il tutto seguendo specifiche architetturali standard già definite anche dal punto di vista tecnologico. L'architettura a *layer* si traduce facilmente in un modello di integrazione tecnologica.

Figura 16. Architettura a layer indipendenti

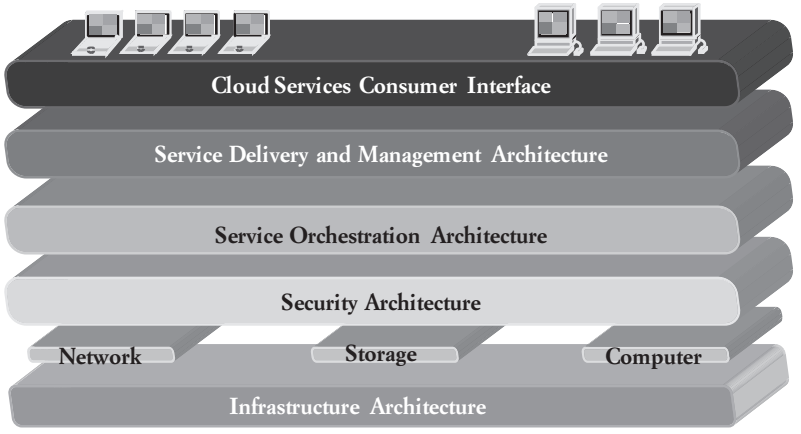


Figura 17. I layer tecnologici

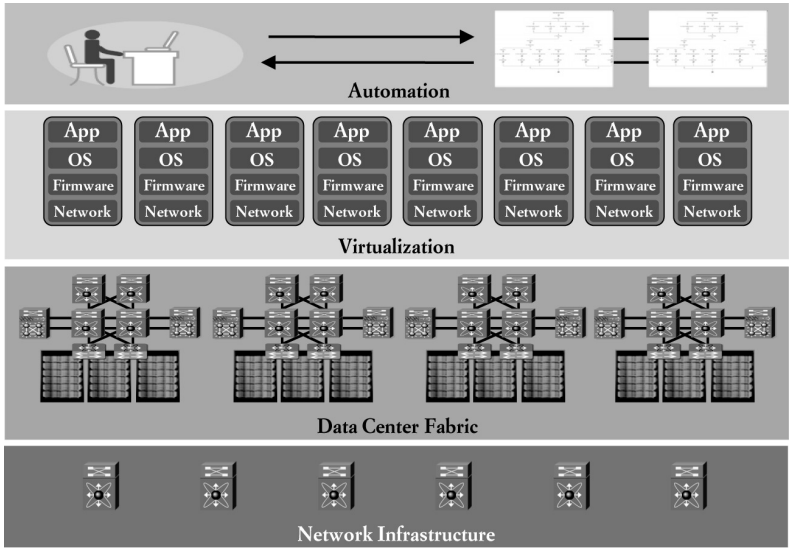
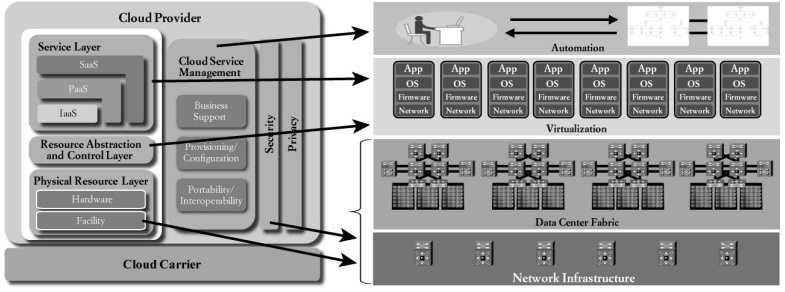
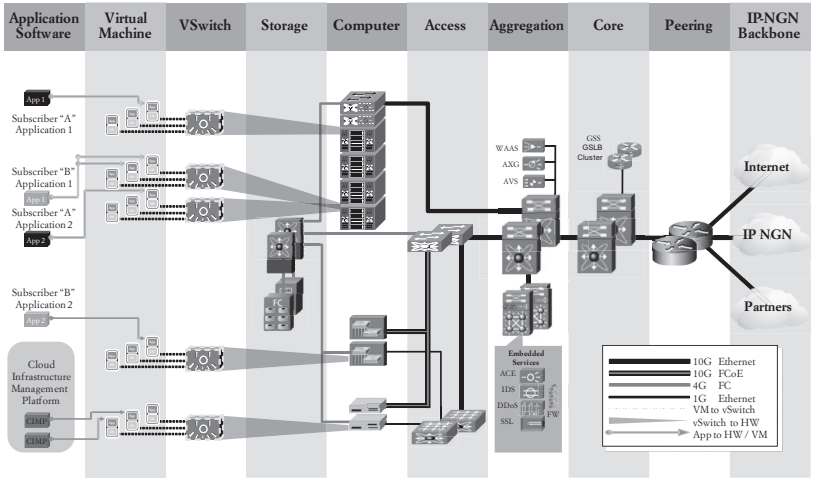


Figura 18. Funzioni e architettura tecnologica



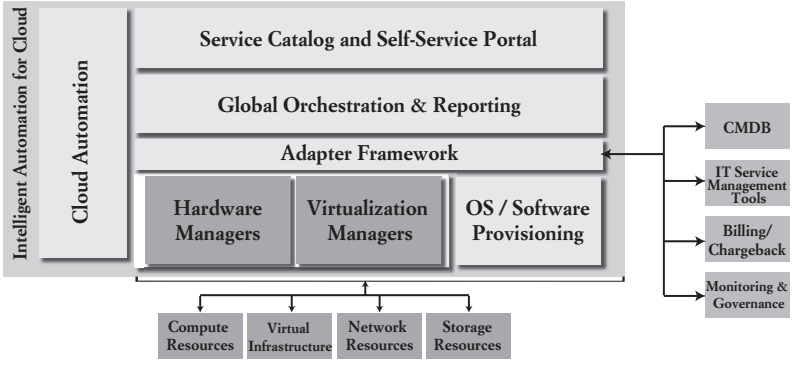
La riconduzione delle esigenze funzionali e della struttura incrementale dei *requirements* è garantita e tutelata dalla stessa architettura tecnologica, che a sua volta garantisce la possibilità di integrazione e di *provisioning* indipendente per livello. Questo significa rendere disponibile un modello architetturale di *provisioning* siffatto:

Figura 19. Il modello di erogazione



Il modello permette inoltre di incrementare progressivamente un portafoglio servizi a cui attingere in logica di *self–provisioning* secondo il modello del *service catalogue* su base Itil[1].

Figura 20. Il modello di provisioning su *service* catalogue



La filiera in questo modo diventa completa:

– i requisiti vengono definiti sulla base delle esigenze funzionali su livelli indipendenti;

– l'architettura *cloud* permette di soddisfare le esigenze in modalità *multi-tier* senza particolari requisiti di integrazione;

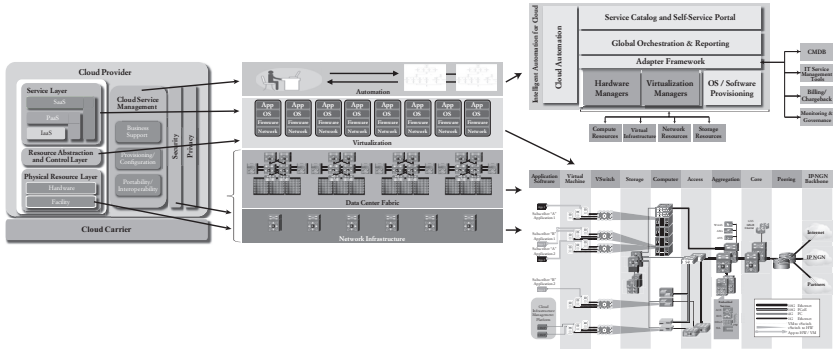
– questo si traduce in:

– un modello di *self-provisioning* a *layer* indipendenti;

– un *service Catalogue* funzionale ad alimentare esigenze analoghe di utenti differenti.

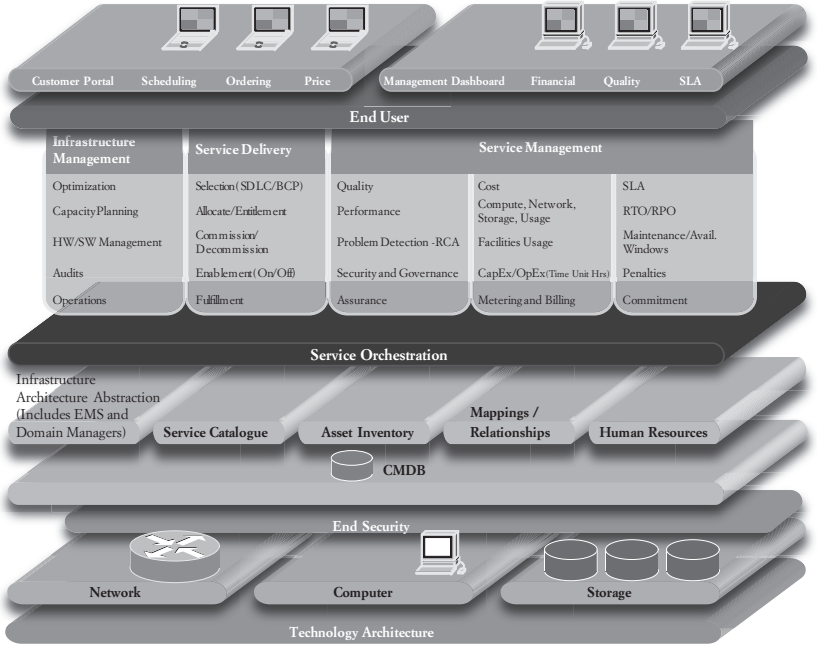
[1] *It Infrastructure Library*.

Figura 21. La catena del valore *cloud-driven*



In questo modo la logica standard di It *service management* su base standard Itil si integra perfettamente col modello di definizione e costruzione dei servizi *cloud*.

Figura 22. *Cloud* e *service catalogue*



In conclusione appare di una certa evidenza come la focalizzazione possa porsi sui diversi livelli dell'architettura, senza che questi si condizionino tra loro né funzionalmente né tecnologicamente, abilitando quelli che sono gli effettivi benefici che il *cloud* può portare anche prescindendo dai puri *savings* economici o dalle classiche logiche di efficienza.

APPENDICE 2

I COSTI PER L'IMPLEMENTAZIONE DEL FASCICOLO SANITARIO ELETTRONICO

1. Scenario conservativo

1.1. Costi di implementazione

Tabella 4. Costi per l'implementazione degli archivi

REGIONE	ARA	AOS	ALA	TOTALE REGIONE
Abruzzi	€ 488.000	€ 260.000	€ 2.160.000	€ 2.908.000
Basilicata	€ 214.000	€ 115.000	€ 2.160.000	€ 2.489.000
Calabria	€ 731.000	€ 390.000	€ 5.400.000	€ 6.521.000
Campania	€ 2.120.000	€ 1.132.000	€ 7.020.000	€ 10.272.000
Emilia Romagna	€ 1.611.000	€ 860.000	€ 9.180.000	€ 11.651.000
Friuli	€ 450.000	€ 240.000	€ 4.320.000	€ 5.010.000
Lazio	€ 2.082.000	€ 1.112.000	€ 10.800.000	€ 13.994.000
Liguria	€ 588.000	€ 315.000	€ 5.400.000	€ 6.303.000
Lombardia	€ 3.605.000	€ 1.925.000	€ 23.760.000	€ 29.290.000
Marche	€ 570.000	€ 305.000	€ 8.640.000	€ 9.515.000
Molise	€ 116.000	€ 62.000	€ 2.160.000	€ 2.338.000
Piemonte	€ 1.620.000	€ 865.000	€ 11.340.000	€ 13.825.000
Puglia	€ 1.487.000	€ 795.000	€ 8.100.000	€ 10.382.000
Sardegna	€ 610.000	€ 325.000	€ 5.400.000	€ 6.335.000
Sicilia	€ 1.835.000	€ 980.000	€ 10.260.000	€ 13.075.000
Toscana	€ 1.365.000	€ 728.000	€ 8.640.000	€ 10.733.000
Trentino	€ 380.000	€ 202.000	€ 2.700.000	€ 3.282.000
Umbria	€ 330.000	€ 175.000	€ 3.240.000	€ 3.745.000
Valle d'Aosta	€ 50.000	€ 25.000	€ 540.000	€ 615.000
Veneto	€ 1.795.000	€ 960.000	€ 12.420.000	€ 15.175.000
TOTALE ITALIA	€ 22.047.000	€ 11.771.000	€ 143.640.000	€ 177.458.000

Tabella 5. Costi delle aziende per l'implementazione del fascicolo

REGIONE	SOFTWARE	ADEGUAMENTO RETE INTERNA	HARDWARE	TOTALE REGIONE
Abruzzi	€ 3.880.000	€ 4.400.000	€ 2.600.000	€ 10.880.000
Basilicata	€ 3.880.000	€ 4.400.000	€ 2.600.000	€ 10.880.000
Calabria	€ 9.700.000	€ 11.000.000	€ 6.500.000	€ 27.200.000
Campania	€ 12.610.000	€ 14.300.000	€ 8.450.000	€ 35.360.000
Emilia Romagna	€ 16.490.000	€ 18.700.000	€ 11.050.000	€ 46.240.000
Friuli	€ 7.760.000	€ 8.800.000	€ 5.200.000	€ 21.760.000
Lazio	€ 19.400.000	€ 22.000.000	€ 13.000.000	€ 54.400.000
Liguria	€ 9.700.000	€ 11.000.000	€ 6.500.000	€ 27.200.000
Lombardia	€ 42.680.000	€ 48.400.000	€ 28.600.000	€ 119.680.000
Marche	€ 15.520.000	€ 17.600.000	€ 10.400.000	€ 43.520.000
Molise	€ 3.880.000	€ 4.400.000	€ 2.600.000	€ 10.880.000
Piemonte	€ 20.370.000	€ 23.100.000	€ 13.650.000	€ 57.120.000
Puglia	€ 14.550.000	€ 16.500.000	€ 9.750.000	€ 40.800.000
Sardegna	€ 9.700.000	€ 11.000.000	€ 6.500.000	€ 27.200.000
Sicilia	€ 18.430.000	€ 20.900.000	€ 12.350.000	€ 51.680.000
Toscana	€ 15.520.000	€ 17.600.000	€ 10.400.000	€ 43.520.000
Trentino	€ 4.850.000	€ 5.500.000	€ 3.250.000	€ 13.600.000
Umbria	€ 5.820.000	€ 6.600.000	€ 3.900.000	€ 16.320.000
Valle d'Aosta	€ 970.000	€ 1.100.000	€ 650.000	€ 2.720.000
Veneto	€ 22.310.000	€ 25.300.000	€ 14.950.000	€ 62.560.000
TOTALE ITALIA	€ 258.020.000	€ 292.600.000	€ 172.900.000	€ 723.520.000

Tabella 6. Costi adeguamento firma

REGIONE	COSTI PER ADEGUAMENTO FIRMA
Abruzzi	€ 10.800.000
Basilicata	€ 10.800.000
Calabria	€ 27.000.000
Campania	€ 35.100.000
Emilia Romagna	€ 45.900.000
Friuli	€ 21.600.000
Lazio	€ 54.000.000
Liguria	€ 27.000.000
Lombardia	€ 118.800.000
Marche	€ 43.200.000
Molise	€ 10.800.000
Piemonte	€ 56.700.000
Puglia	€ 40.500.000
Sardegna	€ 27.000.000
Sicilia	€ 51.300.000
Toscana	€ 43.200.000
Trentino	€ 13.500.000
Umbria	€ 16.200.000
Valle d'Aosta	€ 2.700.000
Veneto	€ 62.100.000
TOTALE ITALIA	€ 718.200.000

Tabella 7. Costi per l'implementazione della extranet

REGIONE	EXTRANET INTEROPERABILITA'	COLLEGAMENTO CON RETE AZIENDE	TOTALE EXTRANET
Abruzzi	€ 3.800.000	€ 4.400.000	€ 8.200.000
Basilicata	€ 3.800.000	€ 4.400.000	€ 8.200.000
Calabria	€ 3.800.000	€ 11.000.000	€ 14.800.000
Campania	€ 3.800.000	€ 14.300.000	€ 18.100.000
Emilia Romagna	€ 3.800.000	€ 18.700.000	€ 22.500.000
Friuli	€ 3.800.000	€ 8.800.000	€ 12.600.000
Lazio	€ 3.800.000	€ 22.000.000	€ 25.800.000
Liguria	€ 3.800.000	€ 11.000.000	€ 14.800.000
Lombardia	€ 3.800.000	€ 48.400.000	€ 52.200.000
Marche	€ 3.800.000	€ 17.600.000	€ 21.400.000
Molise	€ 3.800.000	€ 4.400.000	€ 8.200.000
Piemonte	€ 3.800.000	€ 23.100.000	€ 26.900.000
Puglia	€ 3.800.000	€ 16.500.000	€ 20.300.000
Sardegna	€ 3.800.000	€ 11.000.000	€ 14.800.000
Sicilia	€ 3.800.000	€ 20.900.000	€ 24.700.000
Toscana	€ 3.800.000	€ 17.600.000	€ 21.400.000
Trentino	€ 3.800.000	€ 5.500.000	€ 9.300.000
Umbria	€ 3.800.000	€ 6.600.000	€ 10.400.000
Valle d'Aosta	€ 3.800.000	€ 1.100.000	€ 4.900.000
Veneto	€ 3.800.000	€ 25.300.000	€ 29.100.000
TOTALE ITALIA	€ 76.000.000	€ 292.600.000	€ 368.600.000

Tabella 8. Costi di implementazione totali

REGIONE	COSTI IMPLEMENTAZIONI TOTALI
Abruzzi	€ 32.788.000
Basilicata	€ 32.369.000
Calabria	€ 75.521.000
Campania	€ 98.832.000
Emilia Romagna	€ 126.291.000
Friuli	€ 60.970.000
Lazio	€ 148.194.000
Liguria	€ 75.303.000
Lombardia	€ 319.970.000
Marche	€ 117.635.000
Molise	€ 32.218.000
Piemonte	€ 154.545.000
Puglia	€ 111.982.000
Sardegna	€ 75.335.000
Sicilia	€ 140.755.000
Toscana	€ 118.853.000
Trentino	€ 39.682.000
Umbria	€ 46.665.000
Valle d'Aosta	€ 10.935.000
Veneto	€ 168.935.000
TOTALE ITALIA	€ 1.987.778.000

1.2. Costi annui di gestione e manutenzione

Tabella 9. Costi annui di gestione e manutenzione

REGIONE	GESTIONE AREE CLINICHE	GESTIONE FASCICOLO	INCENTIVI MEDICI	TOTALE REGIONE
Abruzzi	€ 15.200.000	€ 6.557.600	€ 6.712.000	€ 28.469.600
Basilicata	€ 15.200.000	€ 6.473.800	€ 2.937.000	€ 24.610.800
Calabria	€ 38.000.000	€ 15.104.200	€ 10.057.000	€ 63.161.200
Campania	€ 49.400.000	€ 19.766.400	€ 29.170.000	€ 98.336.400
Emilia Romagna	€ 64.600.000	€ 25.258.200	€ 22.162.000	€ 112.020.200
Friuli	€ 30.400.000	€ 12.194.000	€ 6.179.000	€ 48.773.000
Lazio	€ 76.000.000	€ 29.638.800	€ 28.643.000	€ 134.281.800
Liguria	€ 38.000.000	€ 15.060.600	€ 8.084.000	€ 61.144.600
Lombardia	€ 167.200.000	€ 63.994.000	€ 49.588.000	€ 280.782.000
Marche	€ 60.800.000	€ 23.527.000	€ 7.827.000	€ 92.154.000
Molise	€ 15.200.000	€ 6.443.600	€ 1.599.000	€ 23.242.600
Piemonte	€ 79.800.000	€ 30.909.000	€ 22.287.000	€ 132.996.000
Puglia	€ 57.000.000	€ 22.396.400	€ 20.456.000	€ 99.852.400
Sardegna	€ 38.000.000	€ 15.067.000	€ 8.377.000	€ 61.444.000
Sicilia	€ 72.200.000	€ 28.151.000	€ 25.255.000	€ 125.606.000
Toscana	€ 60.800.000	€ 23.770.600	€ 18.749.000	€ 103.319.600
Trentino	€ 19.000.000	€ 7.936.400	€ 5.185.000	€ 32.121.400
Umbria	€ 22.800.000	€ 9.333.000	€ 4.532.000	€ 36.665.000
Valle d'Aosta	€ 3.800.000	€ 2.187.000	€ 641.000	€ 6.628.000
Veneto	€ 87.400.000	€ 33.787.000	€ 24.689.000	€ 145.876.000
TOTALE ITALIA	€ 1.010.800.000	€ 397.555.600	€ 303.129.000	€ 1.711.484.600

Tabella 10. Gestione dotazione medici

REGIONE	GESTIONE DOTAZIONE MEDICI
Abruzzi	€ 3.377.000
Basilicata	€ 1.511.000
Calabria	€ 4.602.000
Campania	€ 13.315.000
Emilia Romagna	€ 9.893.000
Friuli	€ 2.941.000
Lazio	€ 14.953.000
Liguria	€ 4.038.000
Lombardia	€ 20.202.000
Marche	€ 3.806.000
Molise	€ 809.000
Piemonte	€ 10.104.000
Puglia	€ 10.117.000
Sardegna	€ 4.199.000
Sicilia	€ 13.078.000
Toscana	€ 9.019.000
Trentino	€ 2.044.000
Umbria	€ 2.280.000
Valle d'Aosta	€ 309.000
Veneto	€ 10.733.000
TOTALE ITALIA	€ 141.330.000

Tabella 11. Costi di gestione totali

REGIONE	COSTI DI GESTIONE TOTALI
Abruzzi	€ 31.846.600
Basilicata	€ 26.121.800
Calabria	€ 67.763.200
Campania	€ 111.651.400
Emilia Romagna	€ 121.913.200
Friuli	€ 51.714.000
Lazio	€ 149.234.800
Liguria	€ 65.182.600
Lombardia	€ 300.984.000
Marche	€ 95.960.000
Molise	€ 24.051.600
Piemonte	€ 143.100.000
Puglia	€ 109.969.400
Sardegna	€ 65.643.000
Sicilia	€ 138.684.000
Toscana	€ 112.338.600
Trentino	€ 34.165.400
Umbria	€ 38.945.000
Valle d'Aosta	€ 6.937.000
Veneto	€ 156.609.000
TOTALE ITALIA	€ 1.852.814.600

2. Scenario evolutivo

2.1. Costi di implementazione

Tabella 12. Costi di implementazione

REGIONE	PIATTAFORMA UNICA	CHANGE CUP ETC.	CHANGE LABORATORI ETC.	ADEGUAMENTO RETE INTERNA	TOTALE REGIONE
Abruzzi	€ 4.400.000	€ 17.400.000	€ 20.000.000	€ 4.400.000	€ 46.200.000
Basilicata	€ 4.400.000	€ 17.400.000	€ 20.000.000	€ 4.400.000	€ 46.200.000
Calabria	€ 11.000.000	€ 43.500.000	€ 50.000.000	€ 11.000.000	€ 115.500.000
Campania	€ 14.300.000	€ 56.550.000	€ 65.000.000	€ 14.300.000	€ 150.150.000
Emilia Romagna	€ 18.700.000	€ 73.950.000	€ 85.000.000	€ 18.700.000	€ 196.350.000
Friuli	€ 8.800.000	€ 34.800.000	€ 40.000.000	€ 8.800.000	€ 92.400.000
Lazio	€ 22.000.000	€ 87.000.000	€ 100.000.000	€ 22.000.000	€ 231.000.000
Liguria	€ 11.000.000	€ 43.500.000	€ 50.000.000	€ 11.000.000	€ 115.500.000
Lombardia	€ 48.400.000	€ 191.400.000	€ 220.000.000	€ 48.400.000	€ 508.200.000
Marche	€ 17.600.000	€ 69.600.000	€ 80.000.000	€ 17.600.000	€ 184.800.000
Molise	€ 4.400.000	€ 17.400.000	€ 20.000.000	€ 4.400.000	€ 46.200.000
Piemonte	€ 23.100.000	€ 91.350.000	€ 105.000.000	€ 23.100.000	€ 242.550.000
Puglia	€ 16.500.000	€ 65.250.000	€ 75.000.000	€ 16.500.000	€ 173.250.000
Sardegna	€ 11.000.000	€ 43.500.000	€ 50.000.000	€ 11.000.000	€ 115.500.000
Sicilia	€ 20.900.000	€ 82.650.000	€ 95.000.000	€ 20.900.000	€ 219.450.000
Toscana	€ 17.600.000	€ 69.600.000	€ 80.000.000	€ 17.600.000	€ 184.800.000
Trentino	€ 5.500.000	€ 21.750.000	€ 25.000.000	€ 5.500.000	€ 57.750.000
Umbria	€ 6.600.000	€ 26.100.000	€ 30.000.000	€ 6.600.000	€ 69.300.000
Valle d'Aosta	€ 1.100.000	€ 4.350.000	€ 5.000.000	€ 1.100.000	€ 11.550.000
Veneto	€ 25.300.000	€ 100.050.000	€ 115.000.000	€ 25.300.000	€ 265.650.000
TOTALE ITALIA	€ 292.600.000	€ 1.157.100.000	€ 1.330.000.000	€ 292.600.000	€ 3.072.300.000

Tabella 13. Costi per l'implementazione degli archivi

REGIONE	ARA	AOS	TOTALE REGIONE
Abruzzi	€ 488.000	€ 260.000	€ 748.000
Basilicata	€ 214.000	€ 115.000	€ 329.000
Calabria	€ 731.000	€ 390.000	€ 1.121.000
Campania	€ 2.120.000	€ 1.132.000	€ 3.252.000
Emilia Romagna	€ 1.611.000	€ 860.000	€ 2.471.000
Friuli	€ 450.000	€ 240.000	€ 690.000
Lazio	€ 2.082.000	€ 1.112.000	€ 3.194.000
Liguria	€ 588.000	€ 315.000	€ 903.000
Lombardia	€ 3.605.000	€ 1.925.000	€ 5.530.000
Marche	€ 570.000	€ 305.000	€ 875.000
Molise	€ 116.000	€ 62.000	€ 178.000
Piemonte	€ 1.620.000	€ 865.000	€ 2.485.000
Puglia	€ 1.487.000	€ 795.000	€ 2.282.000
Sardegna	€ 610.000	€ 325.000	€ 935.000
Sicilia	€ 1.835.000	€ 980.000	€ 2.815.000
Toscana	€ 1.365.000	€ 728.000	€ 2.093.000
Trentino	€ 380.000	€ 202.000	€ 582.000
Umbria	€ 330.000	€ 175.000	€ 505.000
Valle d'Aosta	€ 50.000	€ 25.000	€ 75.000
Veneto	€ 1.795.000	€ 960.000	€ 2.755.000
TOTALE ITALIA	€ 22.047.000	€ 11.771.000	€ 33.818.000

Tabella 14. Costi per l'implementazione delle extranet

REGIONE	EXTRANET INTEROPERABILITA'	COLLEGAMENTO CON RETE AZIENDE	TOTALE EXTRANET
Abruzzi	€ 3.800.000	€ 4.400.000	€ 8.200.000
Basilicata	€ 3.800.000	€ 4.400.000	€ 8.200.000
Calabria	€ 3.800.000	€ 11.000.000	€ 14.800.000
Campania	€ 3.800.000	€ 14.300.000	€ 18.100.000
Emilia Romagna	€ 3.800.000	€ 18.700.000	€ 22.500.000
Friuli	€ 3.800.000	€ 8.800.000	€ 12.600.000
Lazio	€ 3.800.000	€ 22.000.000	€ 25.800.000
Liguria	€ 3.800.000	€ 11.000.000	€ 14.800.000
Lombardia	€ 3.800.000	€ 48.400.000	€ 52.200.000
Marche	€ 3.800.000	€ 17.600.000	€ 21.400.000
Molise	€ 3.800.000	€ 4.400.000	€ 8.200.000
Piemonte	€ 3.800.000	€ 23.100.000	€ 26.900.000
Puglia	€ 3.800.000	€ 16.500.000	€ 20.300.000
Sardegna	€ 3.800.000	€ 11.000.000	€ 14.800.000
Sicilia	€ 3.800.000	€ 20.900.000	€ 24.700.000
Toscana	€ 3.800.000	€ 17.600.000	€ 21.400.000
Trentino	€ 3.800.000	€ 5.500.000	€ 9.300.000
Umbria	€ 3.800.000	€ 6.600.000	€ 10.400.000
Valle d'Aosta	€ 3.800.000	€ 1.100.000	€ 4.900.000
Veneto	€ 3.800.000	€ 25.300.000	€ 29.100.000
TOTALE ITALIA	€ 76.000.000	€ 292.600.000	€ 368.600.000

Tabella 15. Costi per i medici

REGIONE	DOTAZIONE MEDICI	CARTELLA MEDICI	TOTALE REGIONE
Abruzzi	€ 2.338.000	€ 8.000.000	€ 10.338.000
Basilicata	€ 1.046.000	€ 8.000.000	€ 9.046.000
Calabria	€ 3.186.000	€ 8.000.000	€ 11.186.000
Campania	€ 9.218.000	€ 8.000.000	€ 17.218.000
Emilia Romagna	€ 6.849.000	€ 8.000.000	€ 14.849.000
Friuli	€ 2.036.000	€ 8.000.000	€ 10.036.000
Lazio	€ 10.352.000	€ 8.000.000	€ 18.352.000
Liguria	€ 2.795.000	€ 8.000.000	€ 10.795.000
Lombardia	€ 13.896.000	€ 8.000.000	€ 21.896.000
Marche	€ 2.635.000	€ 8.000.000	€ 10.635.000
Molise	€ 560.000	€ 8.000.000	€ 8.560.000
Piemonte	€ 6.995.000	€ 8.000.000	€ 14.995.000
Puglia	€ 7.004.000	€ 8.000.000	€ 15.004.000
Sardegna	€ 2.907.000	€ 8.000.000	€ 10.907.000
Sicilia	€ 9.054.000	€ 8.000.000	€ 17.054.000
Toscana	€ 6.244.000	€ 8.000.000	€ 14.244.000
Trentino	€ 1.415.000	€ 8.000.000	€ 9.415.000
Umbria	€ 1.579.000	€ 8.000.000	€ 9.579.000
Valle d'Aosta	€ 214.000	€ 8.000.000	€ 8.214.000
Veneto	€ 7.430.000	€ 8.000.000	€ 15.430.000
TOTALE ITALIA	€ 97.753.000	€ 160.000.000	€ 257.753.000

Tabella 16. Costi di implementazione totali

REGIONE	COSTI IMPLEMENTAZIONE TOTALE
Abruzzi	€ 65.486.000
Basilicata	€ 63.775.000
Calabria	€ 142.607.000
Campania	€ 188.720.000
Emilia Romagna	€ 236.170.000
Friuli	€ 115.726.000
Lazio	€ 278.346.000
Liguria	€ 141.998.000
Lombardia	€ 587.826.000
Marche	€ 217.710.000
Molise	€ 63.138.000
Piemonte	€ 286.930.000
Puglia	€ 210.836.000
Sardegna	€ 142.142.000
Sicilia	€ 264.019.000
Toscana	€ 222.537.000
Trentino	€ 77.047.000
Umbria	€ 89.784.000
Valle d'Aosta	€ 24.739.000
Veneto	€ 312.935.000
TOTALE ITALIA	€ 3.732.471.000

Tabella 17. Costi di gestione e manutenzione totali

REGIONE	COSTI GESTIONE TOTALI
Abruzzi	€ 13.097.000
Basilicata	€ 12.755.000
Calabria	€ 28.521.000
Campania	€ 37.744.000
Emilia Romagna	€ 47.234.000
Friuli	€ 23.145.000
Lazio	€ 55.669.000
Liguria	€ 28.400.000
Lombardia	€ 117.565.000
Marche	€ 43.542.000
Molise	€ 12.628.000
Piemonte	€ 57.385.000
Puglia	€ 42.167.000
Sardegna	€ 28.428.000
Sicilia	€ 52.804.000
Toscana	€ 44.507.000
Trentino	€ 15.409.000
Umbria	€ 17.957.000
Valle d'Aosta	€ 4.948.000
Veneto	€ 62.587.000
TOTALE ITALIA	€ 746.492.000

L'IDENTITÀ DIGITALE

1. Il problema

La gestione dell'identità digitale, cioè delle modalità con cui si viene individuati come utenti di servizi erogati in rete da *service provider* pubblici e privati, è un tema non ancora affrontato a livello sistemico: questa situazione di ritardo rappresenta un fattore sia di freno per la diffusione di determinati servizi erogabili in rete sia di difficoltà e complicazione per gli utenti. Affrontare questo tema in modo generale è oggi indifferibile.

Per utilizzare servizi che sempre più frequentemente sono disponibili in rete, e che ormai condizionano la vita quotidiana, attualmente un utente è costretto a servirsi di decine di coppie *userid-password* diverse, cioè di qualcosa che sa, per farsi riconoscere dal sistema informatico del *service provider*. Attualmente ogni *service provider* stabilisce per le *password* regole proprie: quando il servizio richiesto ha necessità di un superiore livello di sicurezza, in aggiunta alle *password*, sono ormai frequentemente utilizzati dispositivi di varia natura, solitamente consegnati personalmente all'utente e capaci di generare l'unica risposta corretta a una domanda proposta a caso dal servizio. Con questo tipo di protocollo, chiamato *challenge/response,* solo chi conosce le *password* ed è anche in possesso del dispositivo (qualcosa che sa e qualcosa che ha), può ottenere l'accesso.

Per gestire gli utenti, i *service provider* hanno la necessità di censirli e di associare a ogni individuo, che desidera utilizzare i loro servizi, uno specifico profilo di utenza: il profilo è costruito quando l'utente accede alla funzione di registrazione del *service provider* e al profilo sono associate le credenziali consegnate all'utente in modo riservato; in genere il profilo è costituito da un insieme di dati e informazioni fornite dall'utente, ma spesso non verificate o verificabili e pertanto il profilo non è collegabile in modo certo a una persona fisica, cioè a un'identità personale. Per molti servizi questo collegamento non è necessario perché il profilo serve al *provider* per

consentire all'utente l'accesso, purché in fase di *login* presenti le credenziali corrispondenti: è sufficiente che l'utente sia riconosciuto dal sistema del *service provider*, dimostrando di conoscere un segreto o di essere in grado di rispondere appropriatamente a una domanda, per consentire l'accesso al servizio.

Nel mondo reale, ai fini di pubblica sicurezza o del diritto a ottenere servizi, le persone sono identificate mediante i loro documenti d'identità personale usati per il riconoscimento a vista (che in pratica significa verificare una caratteristica biometrica del titolare, ad esempio la sua foto). Un documento d'identità è costituito da un insieme d'informazioni e dati certificati da un'autorità e associabili in modo inequivocabile a una persona. Una stessa persona, pur avendo un'unica identità personale, può tuttavia avere più documenti d'identità personale ugualmente validi, rilasciati da autorità pubbliche a ciò preposte per scopi e fini autorizzativi diversi (ad esempio la patente di guida, il passaporto o la carta d'identità). I documenti d'identità personale, pur non essendo tutti equivalenti ai fini autorizzativi, sono validi *erga omnes* per affermare la propria identità.

Per il riconoscimento degli utenti di servizi erogati in rete, è possibile ricreare nel mondo virtuale un identico modello e introdurre documenti d'identità digitale che il titolare, in qualità di persona fisica, potrà utilizzare per asserire nei confronti dei *service provider* la propria identità personale amministrativa e consentirne la verifica: come nel caso reale, lo stesso individuo potrà essere fornito di più documenti d'identità digitale ed è importante che siano realizzati con tecnologie che possano evolvere nel tempo e che li rendano utilizzabili facilmente e in ogni luogo.

I documenti d'identità digitale sono introdotti al solo scopo di consentire l'accesso ai servizi in rete e non è necessario e neppure utile che siano utilizzabili anche per il riconoscimento personale a vista: come dimostra in Italia il caso della carta d'identità elettronica (Cie), il tentativo di unificare, in un dispositivo unico, documenti d'identità personale, finalizzati a esigenze di pubblica sicurezza, e documenti d'identità digitale, finalizzati all'accesso ubiquo ai servizi in rete, non ha avuto successo.

I documenti d'identità digitale sono rilasciati dai *service provider*, in varie forme tecnologiche, a conclusione di una procedura di registrazione e sono il «contenitore» delle informazioni (le credenziali) da presentare ai loro sistemi informatici per ottenere l'accesso ai servizi: per loro natura quindi non possono essere associati con certezza all'identità personale di un individuo; i documenti d'identità digitale sono associati con certezza all'identità personale e amministrativa dell'utente solo se la procedura di registrazione rispetta due condizioni di natura organizzativa e non informatica:

– la procedura deve prevedere una fase in cui l'utente esibisce a un soggetto incaricato di riconoscerlo *de visu*, un documento d'identità personale;

– il documento d'identità digitale rilasciato – che comporta sempre la conoscenza di un segreto – deve essere consegnato con certezza e in modo riservato personalmente all'utente identificato.

È importante chiedersi cosa sarebbe necessario fare per consentire a un utente, dotato di un documento d'identità digitale rilasciato da un determinato *provider*, di utilizzare il medesimo documento per autenticarsi (*login*) ai servizi di qualsiasi altro *service provider,* pubblico o privato.

La sicurezza informatica, prima di essere una caratteristica tecnica, è collegabile ad aspetti organizzativi, di conformità alle norme e agli standard e di rapporti di fiducia (*trust*) tra gli attori. Come avvenuto in casi analoghi (ad esempio quello della firma digitale) è oggi necessario stabilire le regole con cui i documenti d'identità digitale sono rilasciati da soggetti pubblici o privati terzi, che svolgono questo specifico compito in modo conforme a norme di legge e standard tecnici. Se, come avviene ora, i documenti d'identità digitale sono invece rilasciati da ogni *service provider* senza alcuna regolamentazione, diventa insolubile il problema di come si possa stabilire un rapporto fiduciario tra tutti questi soggetti per permettere agli utenti di utilizzare le stesse credenziali per servizi diversi erogati da provider diversi. L'attuale normativa italiana (art. 64 e 65 del nuovo Codice dell'amministrazione digitale – Cad), che pure tratta dei documenti d'identità digitale per l'accesso in rete ai servizi delle amministrazioni pubbliche e della validità delle istanze presentate per via telematica, affronta il tema generale della gestione dell'identità digitale in modo parziale: il risultato è che, allo stato delle cose,

i *service provider* privati e pubblici non accettano o non sono in grado di accettare, documenti d'identità digitale rilasciati da altri *provider*.

In realtà il tema dell'identità digitale non è stato ancora affrontato nei suoi aspetti di natura sistemica e non sono state emanate norme adeguate per regolare la materia: i *provider* si sono perciò comportati in modo autonomo e riconoscono solo le credenziali rilasciate secondo regole proprie. I *provider* pubblici sono confortati in questo comportamento dall'apertura offerta dall'art. 64, comma 2[2], del Cad, che regola le modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni, e anche dalla scarsa diffusione e praticità di uso di della carta d'identità elettronica e della carta nazionale dei servizi, Cie e Cns. La normativa vigente ignora ancora un aspetto fondamentale della gestione dell'identità: per realizzare servizi integrati non è sufficiente, infatti, asserire l'identità nel momento in cui l'utente accede direttamente al servizio, ma le asserzioni d'identità devono essere trasferite anche tra *service provider* in base a relazioni fiduciarie attualmente non regolamentate.

Questo documento si propone di studiare a livello sistemico e infrastrutturale uno schema architetturale e organizzativo per la gestione dell'identità digitale e di proporre aggiornamenti e integrazioni alla normativa vigente, che consentano ai *service provider* di riconoscere e accettare, ai fini identificativi per l'accesso ai propri servizi, anche i documenti d'identità digitale rilasciati da soggetti terzi, che svolgono questo compito in modo conforme a precise norme e regolamenti.

Alle persone fisiche, utenti dei servizi pubblici in rete, dovrebbe essere rilasciato almeno un documento d'identità digitale tecnologicamente fruibile e accettato da tutti i *service provider* pubblici e possibilmente anche da quelli privati: per ottenere questo risultato dovranno essere qualificati e accreditati uno o più soggetti, cui gli utenti potranno rivolgersi per ottenere un documento d'identità digitale, e che avranno il compito di asserirne la validità nei confronti di tutti i *service provider*. Oltre all'impianto normativo e organizzativo, sarà necessario gestire un graduale processo evolutivo che consenta a tutti i *service provider* di accettare, a fini identificativi, nelle fasi di registrazione e di login, i documenti d'identità digitale rilasciati secondo le modalità discusse nei capitoli seguenti.

[2] «Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni».

2. I concetti e i ruoli dell'identità digitale

Ai fini burocratico-amministrativi l'identità personale è verificabile da terze parti confrontando le caratteristiche biometriche del titolare, riscontrabili a vista (o anche mediante sistemi automatizzati) con le informazioni e i dati riportati nei documenti d'identità personale validi, rilasciati da autorità pubbliche. I documenti d'identità personale sono rilasciati per motivi di pubblica sicurezza, o per altri motivi autorizzativi, da autorità pubbliche differenti e possono avere ambiti di applicabilità specifici (ad esempio la patente di guida autorizza a guidare, ma non a espatriare).

L'identità digitale è quell'insieme di dati e informazioni riguardanti l'utente di un servizio erogato in rete che sono raccolti nella fase di registrazione al servizio e che il *provider* utilizza per costruire un profilo di utenza. Tali informazioni comprendono tipicamente dati «identificativi» non verificabili forniti dall'utente stesso e altri dati utili per autorizzare l'accesso al servizio e per comunicare con l'utente, indipendentemente dalla sua identità personale (ad esempio un indirizzo di e-mail o un numero di cellulare). Il profilo di utenza è associato alle credenziali di accesso, che sono l'insieme d'informazioni e dati che il *service provider* consegna in modo riservato agli utenti registrati al servizio, rilasciando un documento d'identità digitale che l'utente presenta nella fase di *login* al sistema informatico esclusivamente per asserire la propria identità. I documenti d'identità digitale, che «contengono» le credenziali, possono essere realizzati con tecnologie diverse e in continua evoluzione, ma in generale sono classificabili, in base alle tipologie di credenziali,

nel modo seguente:

– credenziali basate su qualcosa che l'utente *sa,* oppure qualcosa che *possiede*;

– credenziali basate su qualcosa che l'utente *è*;

– credenziali basate su una combinazione di queste situazioni.

Il processo di *provisioning* è il procedimento organizzativo, amministrativo e informatico con cui il *service provider* crea un profilo d'utenza, genera le credenziali corrispondenti e le consegna in modo confidenziale al titolare in forma di documento d'identità digitale. In funzione delle modalità con cui il processo di *provisioning* è implementato, sarà possibile garantire che il profilo e le credenziali assegnate all'utente siano associate con certezza alla sua identità amministrativa. In questo documento questa caratteristica delle credenziali è chiamata imputabilità. Se le credenziali sono imputabili, il documento d'identità digitale consente, ai fini dell'art. 64, comma 2, del Cad, «l'individuazione del soggetto che richiede il servizio in rete». L'imputabilità non è collegata alla tecnologia con cui sono realizzati i documenti d'identità digitale, ma dipende solo dal processo di *provisioning* che è stato implementato. La tecnologia utilizzata per i documenti d'identità digitale garantisce solo un maggiore o minore grado di sicurezza intrinseca all'uso delle credenziali.

Una stessa persona può quindi avere più documenti d'identità digitale rilasciati direttamente da diversi *service provider*; anche se alcuni *service provider* consegnano agli utenti credenziali imputabili, queste non sono di norma accettate da un altro *service provider*: questo è causa della proliferazione delle credenziali d'accesso, fino a una situazione ingestibile per l'utente. Ciò avviene perché non sono stati adottati standard tecnici, pur esistenti, per un'interazione appropriata tra i sistemi informativi dei *service provider* e perché non esiste una relazione di *trust* tra loro. D'altra parte sarebbe impossibile ipotizzare una relazione fiduciaria tutti a tutti tra *service provider*.

Per affrontare questo problema è necessario definire un modello organizzativo, architetturale, e soprattutto normativo, in cui alcuni *provider*, denominati *identity provider*, si specializzano nei seguenti particolari servizi:

– rilascio di documenti d'identità digitale alle persone che lo richiedono;

– asserzione dell'identità dell'utente ai *service provider* con cui esistono accordi in merito ai livelli d'imputabilità e di sicurezza delle credenziali, e certificazione della veridicità delle informazioni asserite.

Queste relazioni contrattuali e operative tra *service provider* e *identity provider* sono denominate «federazioni». I *service provider* federati, demandano all'*identity provider* i loro compiti d'*identity management*, e l'utente potrà accedere a tutti i loro servizi usando le credenziali ottenute dall'*identity provider*.

Ai fini pratici ed operativi è utile fornire una classificazione degli *identity provider* per tipologia di servizio fornito agli utenti:

– *identity provider*: rilasciano credenziali non imputabili, che non consentono l'accertamento dell'identità personale; ciò non impedisce tuttavia la nascita di federazioni per riutilizzare, presso i *service provider* federati, le credenziali non imputabili ottenute attraverso uno di loro;

– *identity provider qualificati*: rilasciano credenziali imputabili e documenti d'identità digitale qualificati, cioè che possono essere accettati, per l'accertamento dell'identità personale dell'utente, da tutti i *service provider* che fanno parte della Federazione corrispondente.

– *identity provider accreditati*: rilasciano credenziali imputabili e documenti d'identità digitale che devono essere accettati da tutti i *service provider* pubblici e privati che operano sotto la giurisdizione che detta le regole per l'accreditamento: s'introduce così la possibilità per gli utenti di avere almeno un documento d'identità digitale valido *erga omnes*.

Questa classificazione degli *identity provider* si incrocia con le varie tipologie di credenziali che possono essere rilasciate e con i differenti livelli tecnologici di sicurezza e di fruibilità, in funzione del grado di sicurezza richiesto per ogni specifico servizio e anche dei costi di *provisioning* e di gestione.

L'elevato grado di sicurezza dei documenti d'identità digitale è

un ostacolo alla facilità del loro impiego da parte degli utenti e rappresenta quindi un freno alla diffusione dei servizi in rete. Nell'ambito di ogni giurisdizione dovrebbe essere definito un quadro di riferimento sulla sicurezza necessaria all'accesso ai diversi servizi, per non creare da un lato situazioni in cui si richiedono credenziali molto sicure (e costose da rilasciare e gestire) per accedere a servizi o dati che non hanno nessuna particolare esigenza di sicurezza, e dall'altro per consentire un'armonizzazione che eviti che *service provider* diversi richiedano credenziali di livello diverso per servizi analoghi.

Gli *identity provider* accreditati potranno rilasciare documenti d'identità digitale di vario tipo, consentendo uno spettro di possibili livelli di sicurezza in base alle necessità degli utenti. Poiché ai *service provider* pubblici che operano nell'ambito di una stessa giurisdizione sarà richiesto di accettare le asserzioni sull'identità degli utenti indipendentemente dall'*identity provider* utilizzato, purché accreditato, sarà necessario realizzare un registro pubblico, che renda accessibili e verificabili da parte di ogni *service provider* le informazioni sugli *identity provider* accreditati.

3. I dati identificativi e gli attributi dell'identità

Ogni *service provider* costruisce e mantiene un profilo dei propri utenti. Nel caso d'identità digitale imputabile il profilo deve necessariamente contenere i dati personali identificativi certificati. L'insieme minimo dei dati personali identificativi contiene tipicamente le seguenti informazioni: cognome, nome, sesso, data e luogo di nascita ed eventualmente un codice unico.

Per gestire il rapporto con l'utente il *service provider* ha la necessità di raccogliere e mantenere nel suo profilo anche dati personali non identificativi. Si possono distinguere due categorie di dati:

– una prima riguarda informazioni, amministrate dall'utente stesso, che sono necessarie per facilitare i contatti e per personalizzare il servizio, ad esempio un numero di cellulare, una casella di posta elettronica, un indirizzo di recapito, la professione, ecc.

– una seconda comprende informazioni, amministrate invece dal *provider*, che introducono classi differenziate di utenza, generalmente in base a clausole contenute nel contratto di servizio sottoscritto: ad esempio, nell'area dei servizi finanziari, la direttiva comunitaria Mifid impone l'assegnazione a ogni cliente di un profilo di rischio che possa consentire la verifica di adeguatezza delle operazioni d'investimento.

Per molti servizi erogati in rete non è necessario accertare l'identità personale dell'utente; per altri l'accertamento è necessario e sufficiente, per altri ancora l'accertamento dell'identità dell'utente è necessario, ma non sufficiente. In quest'ultimo caso, per autorizzare l'erogazione del servizio richiesto, si dovranno verificare altri attributi della sua identità, che l'utente non può semplicemente asserire personalmente e comunicare al *provider* ma che devono essere certificati da terze parti. Quali dati personali identificativi siano sufficienti per accertare l'identità dell'utente, e quali attributi debbano essere verificati per consentire l'accesso a uno specifico servizio erogato in rete, è funzione del contesto giuridico e amministrativo in cui il *provider* opera. In generale si possono classificare gli attributi in tre categorie: qualifiche, ruoli e deleghe:

– una qualifica (cosa l'utente è) è un'informazione sull'utente del servizio che può essere asserita e certificata solo da soggetti aventi uno specifico titolo di legge, terzi rispetto ai *service provider*, denominati *attribute provider*. Alcuni attributi sono permanenti, ad esempio un titolo di studio acquisito, altri temporanei, ad esempio l'iscrizione a un albo professionale oppure l'abilitazione alla guida (il possesso della patente); un insieme delle qualifiche permanenti potrà essere asserito e certificato anche dagli *identity provider* accreditati prendendo atto, al momento della registrazione dell'utente, *de visu*, di documenti validi (ad esempio un titolo di studio) presentati dalle persone, oppure, ove il servizio sia disponibile, accedendo in rete agli *attribute provider*;

– il ruolo (cosa l'utente può fare) è un'informazione che codifica le autorizzazioni che una persona giuridica concede all'utente per svolgere i compiti che gli sono stati assegnati, qualora l'accertamento della sua identità personale non sia sufficiente per l'erogazione del servizio. Il soggetto che attribuisce il ruolo svolge la funzione di un *identity provider* qualificato, ma limitatamente a specifiche cate-

gorie di persone (ad esempio gli impiegati di un'azienda) ed è responsabile di verificare l'esistenza di eventuali altri attributi necessari per attribuire il ruolo. Una persona può avere più ruoli differenti assegnati dalla stessa o da persone giuridiche diverse;

– la delega è una rappresentazione informatica giuridicamente valida della volontà di una persona (non necessariamente dotata di firma digitale) di conferire a un terzo soggetto, dotato di un documento d'identità digitale accreditato, l'autorizzazione ad accedere, in sua vece, ai servizi di un *service provider*. (Ad esempio il medico di base può utilizzare la propria identità digitale per accedere in rete al fascicolo sanitario elettronico di un proprio assistito, in quanto dispone di una sua delega).

4. Le analogie con l'infrastruttura per la firma digitale

Oggi i *service provider* pubblici e privati gestiscono autonomamente l'identità digitale dei propri utenti e la materia non ha mai ricevuto una adeguata regolamentazione normativa e tecnica.

Non può sfuggire l'analogia del modello descritto con le modalità di rilascio e gestione di dispositivi già introdotti in Italia da oltre dieci anni: la firma digitale, la carta d'identità elettronica e la carta nazionale dei servizi, che rispondono alla definizione data di documenti di identità digitale e che tuttavia non si sono diffusi come era previsto. Ma oggi, soprattutto nell'ottica di un utilizzo di servizi di *cloud computing*, la gestione dell'identità potrebbe trovare in rete un'alternativa più generale, sicura e complessivamente meno costosa.

La classificazione proposta e i compiti attribuiti agli *identity provider*, anche quelli accreditati, non implicano che i loro servizi siano necessariamente forniti da soggetti pubblici. Come già avviene per i Certificatori qualificati e accreditati che rilasciano la firma digitale, anche gli *identity provider* potrebbero essere soggetti privati, che operano in modo conforme ai precisi requisiti di legge. Lo Stato deve quindi promuovere una regolamentazione degli *identity provider* qualificati e accreditati, piuttosto che gestire direttamente un proprio servizio di rilascio di documenti d'identità digitale utilizzabili da tutti i *service provider* del Paese.

È necessario definire il modello architetturale e organizzativo supportato da opportune norme, che definisca l'infrastruttura d'*identity management* del Paese e si possa anche inquadrare nella tendenza più generale di acquisizione in rete di servizi di piattaforma (PaaS) e applicativi (SaaS) abilitata dalle tecnologie del *cloud computing*.

Se si analizza la normativa vigente sulla firma elettronica qualificata, la firma digitale e sui certificatori, qualificati e accreditati[3] si possono confrontare le responsabilità di sicurezza, le garanzie fiduciarie e le procedure di *provisioning* richieste per rilasciare i certificati qualificati e i dispositivi di firma digitale, con le funzioni, le responsabilità e con i compiti che, nel modello proposto, dovrebbero essere attribuiti agli *identity provider* qualificati e accreditati per il rilascio di documenti d'identità digitale e non può sfuggire un'assoluta analogia di ruoli e funzioni. Piuttosto che istituzionalizzare nuovi soggetti, sembrerebbe naturale, quindi, attribuire ai certificatori esistenti, che siano disponibili a svolgerlo, anche questo compito, per il quale sono già attrezzati dal punto di vista organizzativo e dell'infrastruttura tecnologica.

Gli *identity provider* non si limitano tuttavia a rilasciare una tantum documenti d'identità digitale, ma, ogni volta che l'utente accede ad un *service provider* appartenente alla «federazione», sono chiamati ad asserirne l'identità. Questo pone evidenti requisiti di dimensionamento dei loro sistemi e per garantire un adeguato bilanciamento è utile che gli *identity provider*, soprattutto se accreditati, siano in numero sufficiente a garantire prestazioni adeguate. Si può immaginare una situazione a regime in cui si creino delle «federazioni», ad esempio a livello regionale, che possono in ogni caso convivere con *identity provider* a livello nazionale, lasciando agli utenti la scelta di quale documento digitale dotarsi (come avviene per le carte di credito). Peraltro in assenza di un modello sistemico proposto a livello nazionale, alcune regioni già operano come *identity provider* qualificati o accreditati (ad esempio la Regione Lombardia, la

[3] Artt. 26, 27, 28, 29 e 30 del d.lgs. 82/2005 – Codice dell'amministrazione digitale, e successive modifiche e integrazioni apportate dal d.lgs. 30 dicembre 2010, n. 235.

Regione Emilia-Romagna e altre) fornendo ai residenti documenti d'identità digitale e asserendone l'identità agli altri enti locali del territorio.

5. I documenti d'identità digitale e le norme italiane

I documenti d'identità digitale sono «contenitori» che memorizzano le credenziali di accesso a un sistema informatico, con vari livelli di sicurezza che dipendono dalla tecnologia utilizzata.

Il documento d'identità digitale più diffuso, ma anche meno sicuro, è costituito da una coppia di dati (*userid-password*) che il titolare presenta (eseguendo il *login*) al sistema informatico dell'*identity provider* per ottenere l'asserzione d'identità che consente al *service provider* l'attivazione del suo profilo. Si è già argomentato che, se il processo di *provisioning* si è svolto in modo appropriato, anche questo tipo di credenziali può essere imputabile e quindi consentire l'accertamento dell'identità personale dell'utente.

Per aumentare la sicurezza, ma non la facilità di uso, di questa tipologia di credenziali è prassi comune stabilire regole complicate per la password che purtroppo non ne facilitano la memorizzazione, ed in molti casi si richiede anche di modificare la *password* periodicamente. Questi accorgimenti non aumentano di fatto la sicurezza perché gli utenti, di fronte alla numerosità delle proprie credenziali da memorizzare, si difendono scrivendole da qualche parte e anche usando credenziali identiche, o simili, per *provider* differenti. Per circoscrivere questo problema, alcuni portali molto utilizzati, quali ad esempio Google o Facebook, offrono ad altri *service provider* il servizio di asserzione dell'identità degli utenti che sono dotati di loro credenziali, che in genere non sono imputabili.

Il riconoscimento reciproco delle credenziali non è purtroppo attuato dai *service provider* pubblici e privati di maggior interesse per la quotidianità degli utenti, perché manca un rapporto di fiducia nei rispettivi processi di *provisioning* e un coordinamento tra i loro sistemi informativi (tipico il caso dei servizi bancari che richiedono l'uso di credenziali imputabili e documenti d'identità più sicuri).

Per aumentare il livello di sicurezza, le banche distribuiscono oggi agli utenti documenti digitali basati non solo *userid-password*, ma anche su qualcosa che essi hanno assegnando loro dispositivi particolari (tabelle codici, dispositivi Otp, *token* crittografici) che sono in grado di «generare» *password* da usare una sola volta o di indicare a chi li detiene la «risposta» attesa a una «domanda» formulata a caso dal sistema informativo. Questi dispositivi non richiedono l'installazione sul computer dell'utente di hardware o software particolari e quindi, se l'utente li porta con sé, li può usare ovunque accedendo da un qualsiasi computer che non richiede alcuna predisposizione.

Proprio quest'ultimo aspetto si è dimostrato un ostacolo quasi insuperabile alla diffusione dell'uso di credenziali basate su *smart-card* crittografiche, che in teoria sarebbero le credenziali più sicure; tuttavia ancora le recenti modifiche introdotte dal d.lgs. 30 dicembre 2010, n. 235, al Cad ribadiscono che Cie e Cns sono gli strumenti che devono essere accettati da tutte le pubbliche amministrazioni per l'accesso in rete ai servizi che richiedono la «identificazione informatica», ma l'art. 64 non specifica in alcun modo quali essi siano.

La normativa non fornisce peraltro alcun criterio di classificazione dei servizi in base ai requisiti di sicurezza e non prevede la possibilità di utilizzo di strumenti differenziati sulla base dei requisiti di sicurezza di uno specifico servizio. Con l'art. 64, comma 2 si è poi prodotta una norma che, invece di regolamentare adeguatamente la materia anche tenendo conto dell'evoluzione tecnologica, lascia libere tutte le amministrazioni di introdurre qualsiasi altro tipo di «strumento di accesso» purché consenta la «individuazione del soggetto» senza peraltro rimandare ad alcun regolamento che definisca cosa ciò significhi in pratica. In questo modo, tuttavia, si lasciano le amministrazioni (anche il più piccolo Comune) senza direttive tecniche e organizzative per il rilascio di documenti d'identità digitale e del loro livello di sicurezza, perpetuando una situazione di frammentazione difficilmente gestibile per gli utenti finali dei servizi della pubblica amministrazione.

APPENDICE 4

SCHEDE PAESE

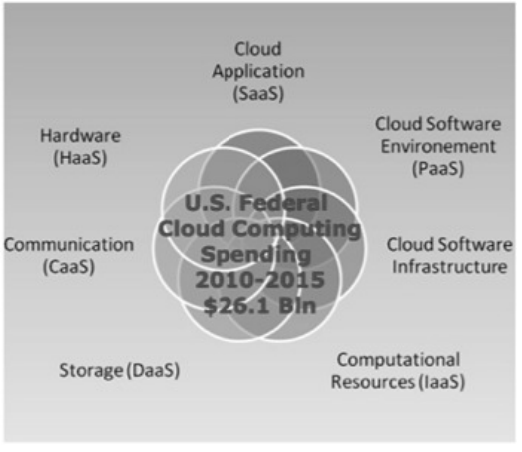
G-*Cloud* negli altri Paesi

Molti tra i principali Paesi (USA, Regno Unito, Australia, Giappone, Singapore, Canada, ecc.) hanno quindi formulato tra il 2010 e il 2011 una strategia per il *cloud computing*.

Nei paesi studiati la strategia, che tipicamente ha un orizzonte temporale decennale, si riferisce innanzitutto alle strutture del governo e quindi alle amministrazioni ed Enti centrali, e in subordine alle amministrazioni ed enti locali.

Il primo passo concreto previsto riguarda solitamente il consolidamento dei *data center* delle amministrazioni centrali e il modello di *governance* è normalmente centralizzato sotto la responsabilità di un *Chief Information Officer* (Cio) o di un'Agenzia che ne svolge le funzioni.

Stati Uniti



Nel 2010 gli Stati Uniti hanno sviluppato la strategia di *cloud computing* federale che ha un orizzonte temporale decennale;

Sviluppati gli standard per il *cloud computing Governance*: Cio Federale

Alcune agenzie statunitensi hanno già adottato con successo tecnologie *cloud*: Defense information sy-

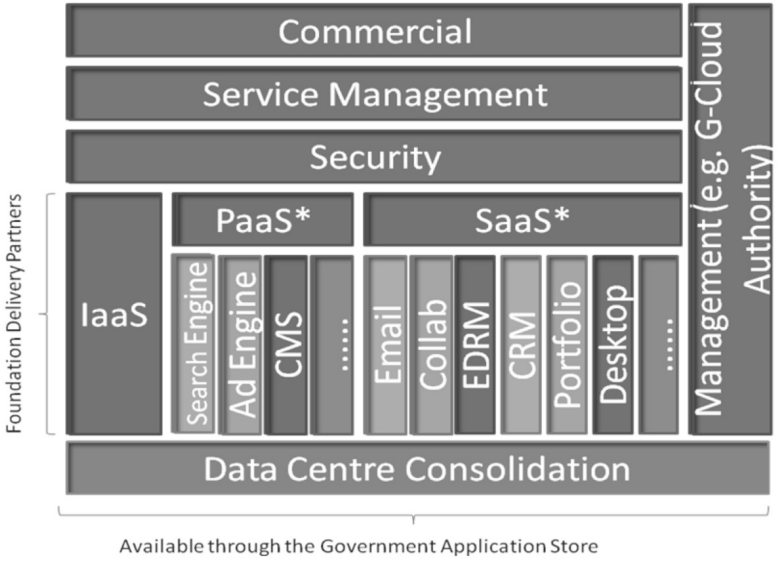
stems agency (Disa): *private cloud* (IaaS). Esempi: Forge.mil, Gcds e Race;

Magellan (gestito dal Dipartimento dell'energia degli Stati Uniti – Doe): *Private Cloud* (IaaS). Questo è stato istituito per determinare la fattibilità del *cloud computing* in termini di costo-efficacia e l'efficienza energetica per gli scienziati al fine di accelerare le scoperte in diverse discipline;

National business center (Nbc) *cloud computing* (gestito dal Ministero degli interni: *private cloud* (IaaS/PaaS/SaaS). Offerta di prodotti di *cloud computing* per i clienti; NBCGrid (IaaS), NBCFiles (cloud *storage*), NBCStage (PaaS), NBC *Hybrid cloud* (consente ai clienti di combinare NBCGrid, NBCFiles con l'infrastruttura esistente), NBCApps, e NBCAuth (SaaS servizio di directory, autenticazione e di prodotto SSO);

NASA Nebula e OpenStack: *Cloud* pubblica (IaaS). Nebula è un pilota *cloud computing* dalla NASA Ames Research Center.

Regno Unito



Il Programma G-*Cloud* è una parte fondamentale della strategia Ict del settore pubblico.

Nel marzo 2011 il governo è passato ad una seconda fase della strategia *cloud*, chiamata G-*Cloud* che prevede il consolidamento dei *data center* e la creazione di un *application store*. La transizione è prevista in 10 anni.

Le singole amministrazioni dovranno eseguire questa transizione in modo coordinato centralmente;

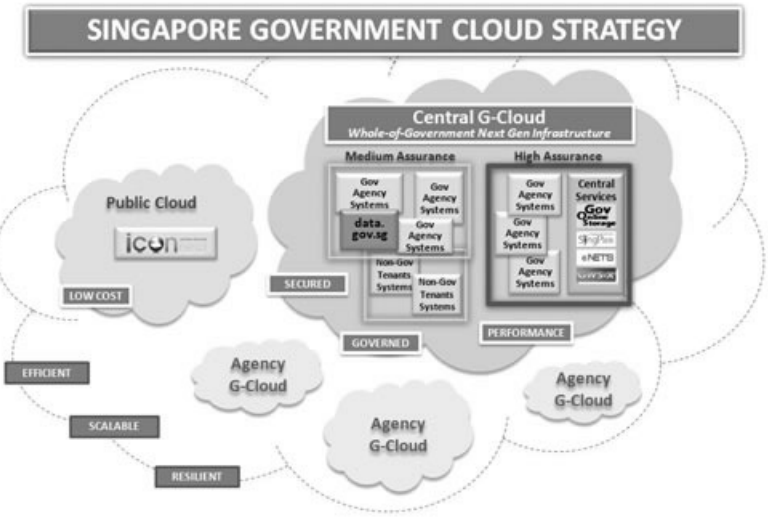
Governance: la *governance* è assicurata da una *G-Cloud Autority*.

Il programma G-*Cloud* dovrebbe fornire i seguenti risparmi:

– £ 300 milioni all'anno (entro il 2015) attraverso il consolidamento dei *data center* in uso nel settore pubblico (ora il costo è pari 5 miliardi di sterline);

– £ 500 milioni all'anno (entro il 2020) grazie alla velocizzazione e maggiore efficacia del processo di appalto tramite l'*application store* per il governo (Asg).

Repubblica di Singapore



Il Piano e-government di Singapore ha previsto un piano di G-*Cloud*, per cui l'intera infrastruttura pubblica (Shine) sarà «claudizzata» per aumentare la competitività e l'economia del paese, secondo un modello multi-polo: adozione del *cloud* pubblico ed implementazione di *cloud* privato per il governo centrale solo per i casi in cui i requisiti di sicurezza e governo non possono essere soddisfatti dal *cloud* pubblico;

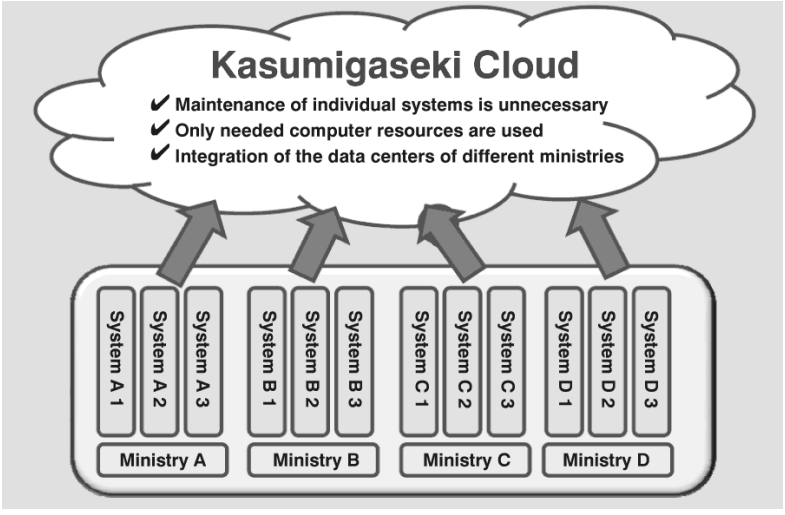
le agenzie governative posso sviluppare le loro «nuvole» solo per rispondere ai bisogni specifici che non possono essere soddisfatti dalle nuvole pubbliche G-*Cloud*;

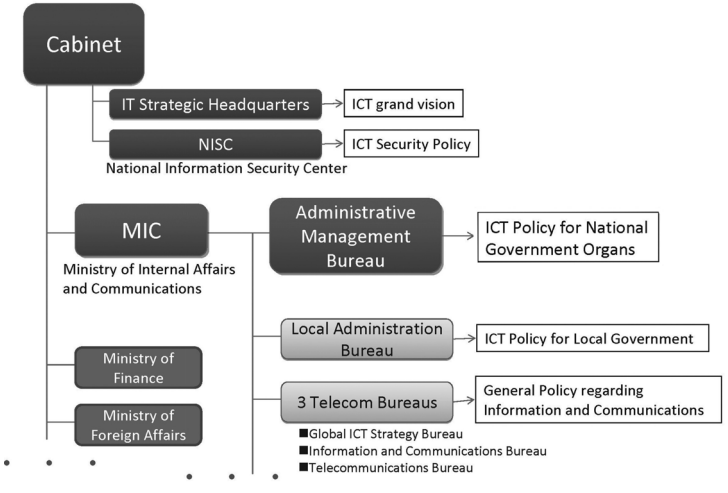
definizione di standard per assicurare l'interoperabilità tra il *cloud* centrale e quello delle Agenzie.

Governance: Singapore ha basato la *governance* sul modello del Cio. È demandata alla Ida (Infocomm Development Authority) che è responsabile della pianificazione, dello sviluppo degli standard, delle linee guida e delle procedure; inoltre gestisce la sicurezza delle infrastrutture critiche.

A marzo 2012, l'Ida aveva già posto in essere 4 bandi per il G-*Cloud*.

Giappone



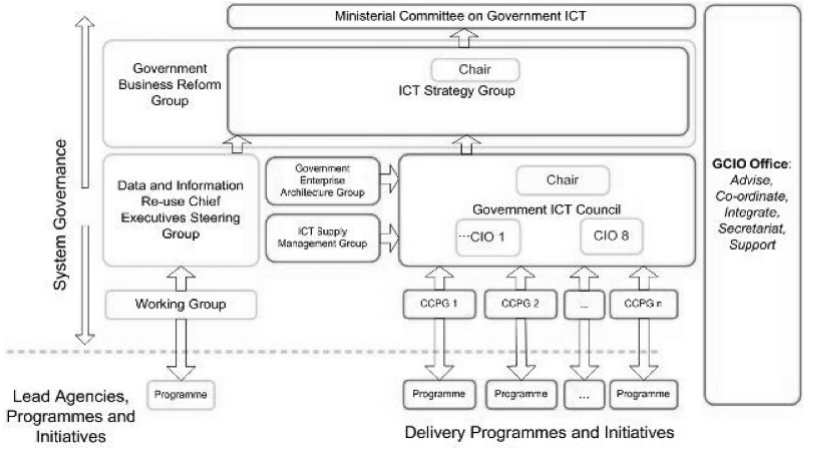


Il Ministero giapponese degli Affari interni e delle Comunicazioni (Mic) ha sviluppato la strategia digitale del Giappone – Digital Japan Creation Project (Ict Piano Hatoyama) – che ha fra gli obiettivi quello di creare nuovi mercati in ambito Ict per rilanciare l'economia del Paese.

Questo piano prevede la creazione di un'ampia infrastruttura nazionale di *cloud computing* privato, il «Kasumigaseki» *cloud*: gli attuali sistemi di *back office*, come la gestione delle buste paga, contabilità e del personale, saranno virtualizzati e ospitati nel *cloud* privato. Alcuni sistemi di *front office*, quali gli appalti elettronici, saranno virtualizzati in un *cloud* pubblico.

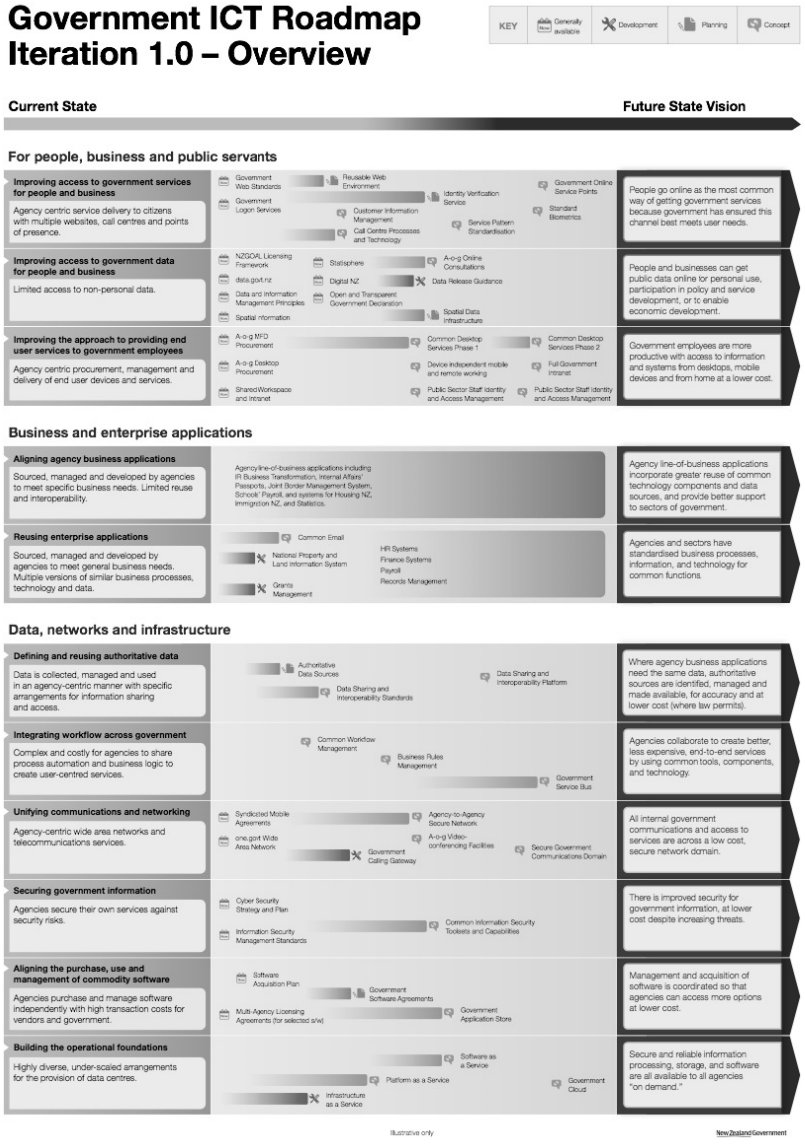
Il piano prevede:
– la completa migrazione nel 2015;
– la costruzione di un Archivio digitale nazionale per la conservazione dei documenti;
– lo sviluppo di cloud *data center green*.

Nuova Zelanda



Il nuovo piano e-government della Nuova Zelanda, lanciato nel 2010, ha previsto come elemento chiave il G-*Cloud*. Il primo passo nello sviluppo della «nuvola» è stato la creazione della infrastruttura nazionale in IaaS, per cui le vari agenzie governative potranno acquistare le proprie infrastrutture informatiche *on demand* che permetterà un risparmio stimato in un forbice da NZ$ 50 milioni (US$ 40 milioni) a NZ$ 250 milioni (US$ 200 milioni) in 10 anni.

Governance: la Nuova Zelanda ha adottato il modello Cio. Per tutta l'infrastruttura pubblica è responsabile un Gcio, che è incardinato nel Ministero degli Affari interni. Nella figura vengono rappresentate le relazioni tra il Gcio e i vari comitati di progettazioni.


Government ICT Roadmap
Iteration 1.0 – Overview
KEY
Generally available
Development
Planning
Concept
Current State
Future State Vision
For people, business and public servants
Improving access to government services for people and business
Agency centric service delivery to citizens with multiple websites, call centres and points of presence.
Government Web Standards
Reusable Web Environment
Government Logon Services
Identity Verification Service
Government Online Service Points
Customer Information Management
Service Pattern Standardisation
Standard Biometrics
Call Centre Processes and Technology
People go online as the most common way of getting government services because government has ensured this channel best meets user needs.
Improving access to government data for people and business
Limited access to non-personal data.
NZGOAL Licensing Framework
Statisphere
A-o-g Online Consultations
data.govt.nz
Digital NZ
Data Release Guidance
Data and Information Management Principles
Open and Transparent Government Declaration
Spatial Information
Spatial Data Infrastructure
People and businesses can get public data online for personal use, participation in policy and service development, or to enable economic development.
Improving the approach to providing end user services to government employees
Agency centric procurement, management and delivery of end user devices and services.
A-o-g MFD Procurement
Common Desktop Services Phase 1
Common Desktop Services Phase 2
A-o-g Desktop Procurement
Device independent mobile and remote working
Full Government Intranet
Shared Workspace and Intranet
Public Sector Staff Identity and Access Management
Public Sector Staff Identity and Access Management
Government employees are more productive with access to information and systems from desktops, mobile devices and from home at a lower cost.
Business and enterprise applications
Aligning agency business applications
Sourced, managed and developed by agencies to meet specific business needs. Limited reuse and interoperability.
Agency line-of-business applications including IR Business Transformation, Internal Affairs' Passports, Joint Border Management System, Schools' Payroll, and systems for Housing NZ, Immigration NZ, and Statistics.
Agency line-of-business applications incorporate greater reuse of common technology components and data sources, and provide better support to sectors of government.
Reusing enterprise applications
Sourced, managed and developed by agencies to meet general business needs. Multiple versions of similar business processes, technology and data.
Common Email
National Property and Land Information System
HR Systems
Finance Systems
Payroll
Records Management
Grants Management
Agencies and sectors have standardised business processes, information, and technology for common functions.
Data, networks and infrastructure
Defining and reusing authoritative data
Data is collected, managed and used in an agency-centric manner with specific arrangements for information sharing and access.
Authoritative Data Sources
Data Sharing and Interoperability Platform
Data Sharing and Interoperability Standards
Where agency business applications need the same data, authoritative sources are identified, managed and made available, for accuracy and at lower cost (where law permits).
Integrating workflow across government
Complex and costly for agencies to share process automation and business logic to create user-centred services.
Common Workflow Management
Business Rules Management
Government Service Bus
Agencies collaborate to create better, less expensive, end-to-end services by using common tools, components, and technology.
Unifying communications and networking
Agency-centric wide area networks and telecommunications services.
Syndicated Mobile Agreements
Agency-to-Agency Secure Network
one.govt Wide Area Network
A-o-g Video-conferencing Facilities
Government Calling Gateway
Secure Government Communications Domain
All internal government communications and access to services are across a low cost, secure network domain.
Securing government information
Agencies secure their own services against security risks.
Cyber Security Strategy and Plan
Common Information Security Toolsets and Capabilities
Information Security Management Standards
There is improved security for government information, at lower cost despite increasing threats.
Aligning the purchase, use and management of commodity software
Agencies purchase and manage software independently with high transaction costs for vendors and government.
Software Acquisition Plan
Government Software Agreements
Multi-Agency Licensing Agreements (for selected s/w)
Government Application Store
Management and acquisition of software is coordinated so that agencies can access more options at lower cost.
Building the operational foundations
Highly diverse, under-scaled arrangements for the provision of data centres.
Software as a Service
Platform as a Service
Government Cloud
Infrastructure as a Service
Secure and reliable information processing, storage, and software are all available to all agencies "on demand."
Illustrative only
New Zealand Government

Accenture S.p.A.

Accenture è un'azienda globale di consulenza direzionale, servizi tecnologici e outsourcing che conta oltre 244 mila professionisti in oltre 120 paesi del mondo. Combinando un'esperienza unica, competenze in tutti i settori di mercato e nelle funzioni di business e grazie ad un'ampia attività di ricerca sulle aziende di maggior successo al mondo, Accenture collabora con i suoi clienti, aziende e pubbliche amministrazioni, per aiutarli a raggiungere alte performance. A livello globale, i ricavi netti per l'anno fiscale 2011 (settembre 2010–agosto 2011) ammontano a 25,5 miliardi di dollari. In Italia è presente con circa 10.500 persone e nell'anno fiscale 2011 ha registrato ricavi netti per 1,029 miliardi di euro. www.accenture.it – www.accenture.com.

Alcatel-Lucent

Partner di eccellenza per service provider, aziende e pubbliche amministrazioni di tutto il mondo, Alcatel-Lucent è leader nell'innovazione nell'ambito delle tecnologie, dei prodotti e dei servizi di comunicazione e networking. Di Alcatel-Lucent fanno parte i Bell Labs, una delle organizzazioni di ricerca e innovazione più all'avanguardia a livello mondiale e culla di molte delle rivoluzioni che hanno ridefinito il settore delle comunicazioni.

Con ricavi per 15,3 miliardi di euro nel 2011, attività in oltre 130 paesi e la struttura di global services più esperta del settore, Alcatel-Lucent è un partner locale su scala mondiale. Alcatel-Lucent ha sede a Parigi.

Cisco Italia

Cisco è presente in Italia dal 1994 e conta circa 700 dipendenti nella sede principale di Vimercate (MI), a Roma, Torino, Padova e Monza, dove ha sede il laboratorio di Ricerca e Sviluppo sulla fotonica.

L'azienda partecipa attivamente allo sviluppo tecnologico del nostro Paese, affiancando imprese, carrier e service provider nella

messa a punto delle loro infrastrutture di rete.

Inoltre, coopera con le amministrazioni pubbliche promuovendo l'adozione e realizzazione di piattaforme tecnologiche efficaci ed efficienti; forte della propria profonda conoscenza delle esigenze della Pa, propone soluzioni per l'e-government, la sicurezza, la comunicazione, l'erogazione di servizi avanzati al cittadino.

CSC

CSC è leader globale nella fornitura di soluzioni e servizi It innovativi in tutti i principali settori di mercato, vantando competenze e referenze all'avanguardia nelle aree Business Solutions & Services e Global Outsourcing Services. Con headquarters a Falls Church (Virginia, USA), CSC è un'azienda di oltre 91.000 persone che nell'anno fiscale chiusosi a aprile 2011 ha fatto registrare ricavi per 16 miliardi di dollari. L'azienda è quotata al New York Stock Exchange con il simbolo «CSC».

L'azienda si avvale della collaborazione di 1.200 professionisti e da febbraio 2007 fa parte della South & West Europe insieme a Francia, Belgio, Lussemburgo, Spagna e Portogallo.

HP

HP crea nuove possibilità affinché la tecnologia abbia un impatto significativo su individui, aziende, istituzioni pubbliche e società. HP, la più grande azienda tecnologica al mondo, dispone di un portafoglio che spazia dalle soluzioni di printing, al personal computing, al software, ai servizi e all'infrastruttura It per risolvere i problemi dei clienti.

IBM Italia

IBM è una società di innovazione al servizio delle aziende e delle istituzioni di tutto il mondo. La sua strategia è quella di costruire e attuare piani di innovazione insieme ai propri clienti e di perfezionare continuamente il portafoglio di offerta per trasferire loro un reale valore di business. IBM detiene da 19 anni il maggior numero di brevetti negli USA e primati in ogni area tecnologica. Inoltre, IBM si rivolge ai clienti con un'offerta in cui le componenti di hardware, software e servizi si armonizzano nel più ampio concetto

di soluzione. L'obiettivo è un'azienda integrata, inserita in un ecosistema costituito da partner, fornitori e clienti in grado di operare con una dinamica struttura a rete per affrontare nuove opportunità, reagire ai cambiamenti, aumentare la flessibilità e accelerare l'esecuzione delle operazioni.

InfoCamere

InfoCamere struttura per la gestione e divulgazione del patrimonio informativo del Sistema Camerale, di cui è parte integrante. Ha realizzato e gestisce il sistema telematico nazionale che collega tra loro le 105 Camere di Commercio. Dal portale www.registroimprese.it si può accedere alle principali banche dati delle Camere di Commercio e agli strumenti per lo svolgimento delle pratiche telematiche, tra cui la Comunicazione unica d'impresa. InfoCamere ha realizzato, per conto delle Camere di Commercio, l'infrastruttura tecnologica che garantisce il corretto funzionamento degli Sportelli unici per le attività produttive, e in particolare il portale «www.impresainungiorno.gov.it». È l'Autorità di certificazione nazionale che rilascia i certificati digitali delle carte tachigrafiche.

Fastweb

Con 1,6 milioni di clienti, è uno dei principali operatori italiani di telecomunicazioni. La società è attualmente presente in oltre 150 aree metropolitane con una rete in fibra ottica che si estende per oltre 32.800 km sul territorio nazionale. Fastweb è stata la prima azienda al mondo ad utilizzare un modello tecnologico basato su IP per la trasmissione di voce, dati e video con l'impiego della fibra ottica e della tecnologia xDSL. Fastweb offre alle famiglie un'ampia gamma di servizi integrati di telefonia fissa e mobile, internet veloce e televisione, su un unico cavo. Agli utenti business offre servizi avanzati e competitivi in tutti i segmenti del mercato. Nel 2007 Fastweb è entrata a far parte del Gruppo Swisscom che oggi detiene l'intero capitale dell'azienda.

Microsoft Italia

Microsoft Italia è parte integrante e attiva dell'area Western Europe di Microsoft. Fondata nell'ottobre del 1985, la filiale dell'a-

zienda di Redmond è presente sul territorio italiano con tre sedi principali, a Milano, Roma e Torino. Conta oltre 850 dipendenti con un'età media di circa 38 anni e 25mila aziende partner. È anche grazie a loro che la filiale italiana di Microsoft è diventata uno dei protagonisti dell'evoluzione informatica e dello sviluppo del nostro Paese, accompagnando milioni di imprese e individui verso l'innovazione tecnologica. In particolare, Microsoft Italia insieme ai suoi partner ha attivato numerosi programmi volti a sensibilizzare aziende e consumatori sui benefici derivanti dalle soluzioni di *cloud computing*.

Oracle Corporation

Presente in oltre 145 paesi nel mondo con 108.000 dipendenti e un fatturato GAAP nell'anno fiscale 2011 pari a 35,6 miliardi di dollari, Oracle Corporation propone la più ampia, completa, aperta e integrata offerta di sistemi software e hardware e vanta oggi oltre 380.000 clienti.

Nata nel 1977 da un'intuizione di Larry Ellison e quotata al Nasdaq dal 1986, Oracle Corporation basa oggi la propria capacità di innovazione su investimenti pari al 12% del fatturato in Ricerca e Sviluppo, area in cui operano attualmente 30.000 sviluppatori e ingegneri.

L'azienda fa leva su più di 20.000 business partner a livello mondiale, cui dedica uno specifico programma, denominato Oracle Partner Network (OPN) Specialized, a garanzia di un supporto continuativo ed efficiente.

Telecom Italia

Telecom Italia offre infrastrutture e piattaforme tecnologiche che abilitano servizi di telecomunicazioni avanzati e soluzioni Ict e media all'avanguardia, con i marchi Telecom Italia, TIM, Virgilio, La7, MTV Italia e Olivetti, supportati nell'innovazione dall'attività di ricerca dei laboratori TILab. Il Gruppo vanta una significativa presenza sul mercato sudamericano con Tim Brasil e Telecom Argentina. Per favorire lo sviluppo digitale del Paese, in particolare nel settore della Pa, Telecom Italia offre soluzioni che spaziano dalla sanità digitale alla dematerializzazione fino alla gestione intelligente del territorio attraverso gli Smart Services; tali servizi sono resi disponibili in modalità «as a service» attraverso la piattaforma evoluta di *cloud computing* della Nuvola Italiana.

Autori

Enrico Acquati, Direttore della ricerca THINK!, già responsabile delle attività di marketing e pianificazione pubblica amministrazione in Honeywell e direttore della ricerca presso IDC Italia, dove si è occupato di ricerche di mercato e consulenza nell'ambito dell'Ict.

Franco Bassanini, Professore di Diritto costituzionale nell'Università di Roma «La Sapienza»; Presidente della Fondazione Astrid; Presidente della Cassa depositi e prestiti, già Ministro della Funzione pubblica nei governi Prodi I, D'Alema II e Amato II (1996-2001).

Miranda Brugi, Esperta senior di e-government, già dirigente del Sistema informativo e reti tecnologiche del Comune di Siena e professore a contratto di Sistemi informativi per la Pa nell'Università di Padova.

Fabrizio Di Mascio, Professore a contratto di Scienza dell'amministrazione nell'Università di Viterbo.

Simona Macellari, Consulente senior di THINK!; Avvocato con specializzazione in diritto pubblico dell'economia e diritto costituzionale italiano e comparato. Già manager Emea di Financial Insights – IDC – e Practice Manager Finance per il Sud Europa di IDC.

Luciano Martucci, Consigliere di THINK!, vanta una lunga esperienza nel mondo dell'information technology, dopo una lunga carriera in IBM è diventato Presidente di IBM Italia fino al 2009. Nel frattempo ha ricoperto cariche in Assolombarda, ed è Senior advisor di Advent International.

Roberto Masiero, Presidente di THINK!, già Presidente di IDC Emea e poi di IDC International dove è stato responsabile del-

le operazioni sul mercato internazionale e delle attività di government relations, con focus sui temi dell'innovazione, delle tecnologie digitali per lo sviluppo e dei mercati emergenti.

Alessandro Natalini, Componente della CIVIT; docente di Scienza dell'amministrazione nell'Università Parthenope di Napoli; già membro del Nucleo per la semplificazione (1999-2002) e dell'Unità per la semplificazione presso la Presidenza del Consiglio dei ministri (2006-2007).

Carlo Notarmuzi, Dirigente generale della Presidenza del Consiglio dei ministri; Direttore della Segreteria tecnica dell'Unità per la semplificazione e la qualità della regolazione.

Alessandro Osnaghi, Direttore Area pubblica amministrazione di THINK! e socio Astrid; già consigliere del Ministro per la Funzione pubblica per il Piano d'azione e-government 2000, direttore del Centro tecnico Rupa e dirigente della Autorità per l'informatica nella pubblica amministrazione. È stato Professore associato nell'Università di Pavia e nell'Università di Milano.

Rosario Piazzese, Consulting Director di THINK!, opera nel *management* consulting da più di 20 anni, prima come manager in grandi realtà internazionali, poi come socio o fondatore di nuove realtà della consulenza italiana (TIG, ISAS Group).

Jacopo Sce, Direttore della Fondazione Astrid.

Contributori

Marco Amabile, Accenture. Senior Manager nel settore di mercato «Health & Public service» specializzato nella consulenza direzionale alle pubbliche amministrazioni per l'analisi di policy, la definizione di strategie e la progettazione, realizzazione e manutenzione di sistemi su vasta scala.

Giuseppe Buono, Accenture. Senior Manager di It Strategy, Infrastructure & Security (ISIS), è oggi focalizzato su tematiche di *Cloud Strategy* & *Transformation* ed impegnato in progetti di adozione del paradigma *cloud* per aziende private e pubblica amministrazione.

Massimo Cannizzo, Accenture. Senior Executive responsabile It Strategy consulting per Italia, Est Europa e Medio Oriente. Copre il ruolo di responsabile di grandi progetti di trasformazione ed innovazione dell'Ict, su tematiche sia tecnologiche sia organizzative.

Claudio Coltro, Alcatel-Lucent. Responsabile Marketing e Strategia per soluzioni *cloud computing* e CDN nel mercato Emea per Alcatel-Lucent, coprendo aspetti di business development, business analysis e soluzioni.

Andrea Maria Nicola Costa, Telecom Italia. Responsabile per Telecom Italia del progetto EXPO 2015. Dal febbraio 2010 al dicembre 2011 responsabile Marketing per la Business Unit Public Sector di Telecom Italia con competenza su soluzioni per il territorio, la sanità, la burocrazia digitale.

Gianfilippo D'Agostino, Telecom Italia. Attualmente responsabile della direzione Sales nell'ambito della funzione Top Clients and Public Sector, dopo essere stato Direttore della Business Unit Public Sector di Telecom Italia. È Presidente della Sezione Comunicazioni Unindustria Roma e Vice presidente Gruppo Merceologico Telecomunicazioni Assolombarda.

Pier Luigi Dal Pino, Microsoft. Direttore centrale per le Relazioni istituzionali e industriali di Microsoft Italia, rappresenta il principale referente italiano dedicato ai rapporti istituzionali in ambito politico e regolamentare. Da oltre 9 anni Direttore dei Rapporti istituzionali di Microsoft Italia, di cui 4 anni con responsabilità per il Sud Europa.

Sefano Devescovi, IBM. È Public Sector Industry Leader di IBM Italia. Ingegnere, con alle spalle esperienze professionali sia in Italia che all'estero, ha sviluppato le sue competenze nelle aree della pubblica amministrazione, e-government, public procurement e progetti di trasformazione di tipo sistemico.

Claudio Di Genova, Fastweb. È Public Sector Agreements Specialist della Business Unit Enterprise. Lavora in Fastweb dal 2006, dove ha precedentemente svolto il ruolo di Key Account Manager sia nel settore pubblica amministrazione che in quello Grandi Aziende.

Giuseppe Di Natale, HP. Con 25 anni di esperienza in Ict, contribuisce alla realizzazione della Rupa, l'attuale Spc, nonché ai principali contratti di outsourcing in Italia, dove per HP è oggi responsabile dello sviluppo del business strategico.

Fabio Di Vita, Oracle. Technical Account Sales Consultant a Oracle Corporation.

Sergio Fiora, Oracle. Business Development Public Sector.

Fabrizio Gergely, Cisco. Manager Systems Engineering Public Sector Italy. In Cisco Systems dall'inizio del 2000 come Systems Engineer, ha svolto il ruolo di Vertical Solution Architect, per poi prendere la responsabilità del Team di Systems Engineering per il Public Sector in Italia. Precedentemente ha lavorato in Telecom Italia e Vitrociset. Laureato in Ingegneria elettronica presso l'Università Roma «Tor Vergata».

Marco Giletta, HP. Consulting Director Public Sector a livello Emea. Ha sviluppato una consolidata esperienza anche a livello internazionale, attraverso esperienze maturate presso multinazionali Ict e società di consulenza direzionale.

Giuseppe Gorla, Accenture. Senior Executive responsabile Technology consulting e Infrastructure Outsourcing per Italia, Est Europa e Medio Oriente. Copre il ruolo di responsabile della divisione e della conduzione di selezionati progetti con alto contenuto di innovazione.

Remo Gozzi, HP. Business Development Manager Public Sector. Con una lunga esperienza sia nel pubblico che nel privato, ha in passato svolto ruoli di Direzione generale, CIO, consulente di Direzione, e Responsabile di progetti strategici.

Carlo Iantorno, Microsoft. National Technology Officer di Microsoft in Italia, all'interno della divisione Public Sector. Responsabile della strategia e policy tecnologiche, nell'ambito del piano di sviluppo nazionale di Microsoft per l'Italia.

Massimo Leoni, IBM. Lavora in IBM Italia come responsabile della progettazione di infrastrutture It per primari gruppi bancari italiani. Laureatosi in ingegneria ha poi sviluppato le sue competenze nelle aree della sicurezza, integrazione applicativa e analisi prestazionale.

Rosita Mainieri, IBM. Si occupa di sviluppare l'adozione di modelli architetturali e di servizio basati sul *cloud computing* presso alcuni importanti clienti IBM in Italia.

Paolo Massafra, Cisco. Sales Business Development Manager. Dopo l'attività di ricerca presso l'università e Telecom Italia Labs, nel 1997 passa in Cisco, ricoprendo diversi ruoli e incarichi. Dal 2009 passa nella struttura Emea come Strategic Alliance Manager sul Gruppo Finmeccanica.

ENRICO MERCADANTE, Cisco. Business Development Manager, responsabile per Cisco Systems dello sviluppo del mercato *cloud* e *Managed Services* nel Sud Europa dal 2010. In Cisco dal 2000, dopo un'esperienza di Product Manager in Ericsson a Stoccolma. Laureato in Ingegneria delle telecomunicazioni presso l'Università «La Sapienza» di Roma.

FRANCO MICOLI, Alcatel-Lucent. Responsabile Relazioni Istituzionali, si occupa di promuovere la visione di Alcatel-Lucent e supportare la valorizzazione di tecnologie e servizi digitali innovativi presso policy maker e stakeholders di mercato.

ANTONELLO MILÌA, IBM. Lavora in IBM Italia come Industry Architect per il settore pubblico locale. Laureato in ingegneria, ha collaborato presso importanti aziende multinazionali occupandosi della realizzazione di progetti web per aziende italiane e straniere di differenti settori.

FEDERICO MORENA, Telecom Italia. Product Manager nell'ambito del Marketing di Telecom Italia – Top Clients and Public Sector, con specifica responsabilità nelle soluzioni per la dematerializzazione e l'efficientamento dei processi attraverso piattaforme *cloud based*.

ALESSANDRO MOSCARDELLI, Accenture. Senior Executive di Accenture. Responsabile Advenced Systems and Technology (AS&T) per la pubblica Amministrazione. È oggi focalizzato su complessi programmi di rinnovamento ed evoluzione tecnologica per grandi enti pubblici.

STEFANO PAMBIANCHI, Cisco. Direttore Italia della divisione internet Business Solutions, che supporta le top aziende nel migliorare le performance business e strategie competitive, grazie alle nuove tecnologie. Prima di entrare in Cisco, ha lavorato per 11 anni in Booz Allen Hamilton, dove ha sviluppato la practice consumer e Retail in Italia, Europa e Middle East.

GENNARO PANAGIA, IBM. Ha la responsabilità in Italia dell'offerta *cloud computing* per IBM Global Technology Services. In precedenza ha guidato la divisione servizi dedicata alle infrastrutture It e la direzione vendite della divisione servizi It infrastrutturali per i principali settori di industria.

GIUSEPPE PATTI, CSC. Business Developper Executive.

GIAN LUCA PETRILLO, Microsoft. Government Affairs Manager. Responsabile delle Relazioni istituzionali lavora con il Parlamento, il governo e le regioni sulle normative e programmi di governo che hanno impatto sull'innovazione tecnologica e sul business di Microsoft. Mantiene relazioni con il Parlamento europeo e la Commissione europea, coordinandosi con le funzioni interne di Bruxelles.

MAURIZIO POERIO, CSC. Insitutional Relations director.

STEFANIA POMPILI, CSC. In CSC dal 2005, ricopre il doppio ruolo di Government & Services B.U. Director e Rome Site Managing Director. Ricadono sotto la sua responsabilità gli aspetti commerciali e di delivery sia dei mercati di riferimento sia degli uffici di Roma.

ENRICO PROSERPIO, Oracle. Senior Technology Director Sales Consulting. È responsabile di tutto il team Technology per l' Italia ede' inoltre leader per il sud Europa. In Oracle si occupa di *cloud computing*, collaborando con il Product *management* e con le strutture europee dedicate a queste aree.

EMIDIO ROMANO, Fastweb. È Public Sales Agreements Manager della Business Unit Enterprise di Fastweb dove è responsabile degli accordi quadro che fanno capo a Consip e DigitPa e dello sviluppo dei relativi servizi. Ingegnere elettronico, ha avuto precedenti esperienze in Telecom Italia.

MIRKO SANTOCONO, Fastweb. È Marketing Product Manager della Business Unit Enterprise dove si occupa di offerta commercia-

le dei servizi di *cloud computing*, *data center*, *unified communications*, Ict Security. Ingegnere delle telecomunicazioni, ha avuto precedenti esperienze lavorative in Italtel, General Motors Europe, Alcatel-Lucent, SFR.

ROBERTO SCRIVO, Fastweb. È Responsabile delle Relazioni istituzionali di Fastweb, dove si occupa di attività di lobbying e della gestione dei rapporti istituzionali con governo, Parlamento, regioni, ministeri, organismi, enti ed associazioni di rappresentanza. Laureato in giurisprudenza, ha avuto precedenti esperienze lavorative in Confindustria.

FABIO SPOLETINI, Oracle. Country Leader Technology.

GIUSEPPE VOZZA, Fastweb. È Presale Coordinator della Business Unit Enterprise di Fastweb. Laureato in Ingegneria informatica, ha sviluppato la sua esperienza professionale in ambito Ict, nei mercati Pa e Finance, passando da ambiti prettamente sistemistici, al project management e alla progettazione di servizi sia Core che VAS.

INDICE PARTICOLAREGGIATO

ASTRID

Volumi pubblicati:

Libri di ASTRID, Passigli Editori, Firenze

Costituzione una riforma sbagliata, a cura di Franco Bassanini, 2004

Sviluppo o declino, a cura di Luisa Torchia e Franco Bassanini, 2005

Gli sportelli unici per le attività produttive: fallimento o rilancio?, a cura di Bruno Dente e Franco Bassanini, 2007

La riforma elettorale, di Enzo Cheli, Franco Bassanini, Cesare Pinelli, Stefano Passigli *et al.*, 2007

Semplificare l'Italia. Stato, Regioni, Enti locali, a cura di Franco Bassanini e Luca Castelli, 2008

Dove lo Stato non arriva. Pubblica amministrazione e Terzo settore, a cura di Caterina Cittadino, 2008

Per una moderna democrazia europea. L'Italia e la sfida delle riforme istituzionali, a cura di Franco Bassanini e Roberto Gualtieri, 2009

Governare l'economia globale. Nella crisi e oltre la crisi, a cura di Giuliano Amato, 2009

I nodi delle reti. Infrastrutture, mercato e interesse pubblico, a cura di Paola M. Manacorda, 2010

Il finanziamento dell'Europa. Il bilancio dell'Unione e i beni pubblici europei, a cura di Maria Teresa Salvemini e Franco Bassanini, 2010

La Corruzione amministrativa. Cause, prevenzioni e rimedi, a cura di Francesco Merloni e Luciano Vandelli, 2011

Istruzione bene comune. Idee per la scuola di domani, a cura di Vittorio Campione e Franco Bassanini, 2011

Regioni, Corecom e banda ultralarga, a cura di Paola M. Manacorda e Giovanna De Minico, 2011

Esclusione sociale. Politiche pubbliche e garanzie dei diritti, a cura di Cesare Pinelli, 2012

Studi e Ricerche scelti da ASTRID, Passigli Editori, Firenze

L'Europa legittima. Principi e processi di legittimazione nella costruzione europea, di Nicola Verola, 2006

Dignità umana e Stato costituzionale. La dignità umana nel costituzionalismo europeo, nella Costituzione italiana e nelle giurisprudenze europee, di Mario Di Ciommo, 2010

L'obiezione di coscienza. Studio sull'ammissibilità di un'eccezione dal servizio militare alla bioetica, di Davide Paris, 2011

Paper di ASTRID, Passigli Editori, Firenze

Il sistema radiotelevisivo. Dieci proposte di riforma, a cura di Enzo Cheli e Paola M. Manacorda, 2006

Per un nuovo ordinamento giudiziario, a cura di Elena Paciotti, 2006

La Rai del futuro, di Paolo Gentiloni, Giuliano Amato, Enzo Cheli, Leopoldo Elia *et al.*, 2007

I referendum elettorali, di Giuliano Amato, Gaetano Azzariti, Franco Bassanini, Enzo Bianco *et al.*, 2007

Gli indicatori di competitività dell'economia italiana nel quadro del processo di Lisbona, a cura di Pippo Ranci e Andrea Forti, 2009

Quaderni di ASTRID, edizioni Il Mulino, Bologna

Una Costituzione per l'Europa. Dalla Convenzione europea alla Conferenza Intergovernativa, a cura di Franco Bassanini e Giulia Tiberi, 2003

L'attuazione del federalismo fiscale. Una proposta, a cura di Franco Bassanini e Giorgio Macciotta, 2004

Verso il federalismo. Normazione e amministrazione nella riforma del Titolo V della Costituzione, a cura di Vincenzo Cerulli Irelli e Cesare Pinelli, 2004

La Costituzione europea. Un primo commento, a cura di Franco Bassanini e Giulia Tiberi, 2004

Welfare e federalismo, a cura di Luisa Torchia, 2005

Verso l'Europa dei diritti. Lo Spazio europeo di libertà, sicurezza e giustizia, a cura di Giuliano Amato e Elena Paciotti, 2005

I tempi della giustizia. Un progetto per la riduzione dei tempi dei processi civili e penali, a cura di Elena Paciotti, 2006

Università e sistema della ricerca. Proposte per cambiare, a cura di Marco Cammelli e Francesco Merloni, 2006

Le virtù della concorrenza. Regolazione e mercato nei servizi di pubblica utilità, a cura di Claudio De Vincenti e Adriana Vigneri, 2006

Lo Stato compratore. L'acquisto di beni e servizi nelle pubbliche amministrazioni, a cura di Luigi Fiorentino, prefazione di Franco Bassanini, 2007

Per far funzionare il Parlamento. Quarantaquattro modeste proposte, a cura di Andrea Manzella e Franco Bassanini, 2007

L'amministrazione come professione. I dirigenti pubblici fra spoils system e servizio ai cittadini, a cura di Gianfranco D'Alessio, 2008

Le nuove istituzioni europee. Commento al Trattato di Lisbona, a cura di Franco Bassanini e Giulia Tiberi, 2008

La riforma del welfare. Dieci anni dopo la "Commissione Onofri", a cura di Luciano Guerzoni, 2008

La sfida dell'energia pulita. Ambiente, clima e energie rinnovabili: problemi economici e giuridici, a cura di Alfredo Macchiati e Giampaolo Rossi, 2009

Arbitri dei mercati. Le Autorità indipendenti e l'economia, a cura di Marco D'Alberti e Alessandro Pajno, 2010

La costituzione economica: Italia, Europa, a cura di Cesare Pinelli e Tiziano Treu, 2010

La tela di Penelope. Primo Rapporto Astrid sulla semplificazione legislativa e burocratica, a cura di Alessandro Natalini e Giulia Tiberi, 2010

La sanità in Italia. Organizzazione, governo, regolazione, mercato, a cura di Claudio De Vincenti, Renato Finocchi Ghersi e Andrea Tardiola, 2011

Gli acquisti delle amministrazioni pubbliche nella Repubblica federale, a cura di Luigi Fiorentino, 2011

Ricerche di ASTRID, Il Sole-24 Ore, Milano

La salute e il mercato. La ricerca farmaceutica tra Stato, industria e cittadini, a cura di Giorgio Macciotta, 2008

Libri di ASTRID, Maggioli Editore, Rimini

La sicurezza urbana, a cura di Alessandro Pajno, 2010

I servizi pubblici locali tra riforma e referendum, di Claudio De Vincenti e Adriana Vigneri, 2011