Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE

Ciclo XXVIII

Settore Concorsuale di afferenza: 12/H3

Settore Scientifico disciplinare: IUS/20

Il *cloud computing* in ambito sanitario

Presentata da: Massimo Farina

Coordinatore Dottorato

Prof. Giovanni Sartor

Relatore

Prof. ssa Carla Faralli

Correlatore

Dott.ssa Raffaella Brighi

Esame finale anno 2016

INDICE

ABBREVIAZIONI

AgID	Agenzia per l'Italia Digitale
AO	Azienda Ospedaliera
API	Application Programming Interfaces
ASL	Azienda Sanitaria Locale
AWS	Amazon Web Services
BCR	Binding Corporate Rules
CED	Centro Elaborazione Dati
CIO	Chief Information Officer
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
DLP	Data Loss Prevention
DOS	Denial of Service
EHR	Electronic Health Record
ENISA	European Union Agency for Network and Information Security
EPR	Electronic Patient Record
FSE	Fascicolo sanitario elettronico
GAE	Google App Engine
GEPD	Garante europeo della protezione dei dati
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICD	International Classification of Diseases
IdP	Identity Provider
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IPS/IDS	Intrusion Prevention and Detection System
ISMS	Information Security Management System
ISO	International Standards Organisation

ISV	Independent Software Vendor
LAN	Local Area Network
MIT	Massachusetts Institute of Technology
NAC	Network Admission Control
NIST	National Institute for Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PaaS	Platform as a Service
PACS	Picture archiving and communication system
PDA	Personal Digital Assistant
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SDO	Scheda di Dimissione Ospedaliera
SLA	Service Level Agreement
SoA	Service Oriented Architecture
STP	Spanning Tree Protocol
UML	Unified Modeling Language
VM	Virtual Machines (macchine virtuali)
VPN	Virtual Private Network
WAH	Windows Azure Hypervisor
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

INDICE DELLE FIGURE

INTRODUZIONE

1.1 Contesto di riferimento

L'evoluzione tecnologica in ambito IT impone alle aziende pubbliche e private di stare al passo con i tempi e conduce verso un continuo aggiornamento di mezzi e risorse. L'assenza di innovazione, infatti, può essere altamente penalizzante, soprattutto se l'uso di risorse tecnologiche e di sistemi informatici è vitale, come in molti settori della Pubblica Amministrazione (ormai indirizzata verso la totale digitalizzazione).

In un contesto di piena evoluzione tecnologica, altamente competitivo, fin dagli anni '90 si è assistito a una ricerca di interazione tra diversi e distanti sistemi di elaborazione al fine di ottenere una cooperazione a livello computazionale tale da riuscire a svolgere calcoli (e quindi erogare servizi) impensabili nel singolo contesto tecnologico aziendale.

La tecnologia che risponde a questo tipo di esigenze è il *cloud computing* che porta la computazione e i dati fuori dal contesto aziendale, quindi in luoghi lontani dalle macchine *client*, verso grandi *data centers*. Con il *cloud computing* si utilizzano e si combinano risorse distribuite per raggiungere un *throughput* più elevato e risolvere problemi computazionali su larga scala.

La diffusione della computazione "nuvolare" ha coinvolto ogni settore di elaborazione delle informazioni digitali, compreso quello sanitario (pubblico e privato), comportando un mutamento di approccio rispetto alla visione tradizionale del rapporto tra l'assistito e il servizio sanitario. I più evidenti cambiamenti di tale paradigma si notano in riferimento alle modalità di accesso e fruizione dei servizi di assistenza, ai processi di prevenzione e cura, nonché alle nuove modalità operative del personale sanitario (medico di medicina generale, pediatra di libera scelta e specialista).

Tale processo di ammodernamento della sanità ha dato luogo allo sviluppo di numerose iniziative[1] finalizzate al miglioramento dell'efficienza dei servizi sanitari e legate ad una gestione sempre più ampia di atti, documenti e procedure, attraverso modalità informatiche e telematiche.

Il *Cloud Computing*, in ciascuna delle sue forme, rappresenta l'evoluzione ulteriore del processo di digitalizzazione nella gestione amministrativa della sanità, portando numerosi benefici. Si consideri, in tal senso, in primo luogo, il contenimento dei costi (ribaltati sul *cloud provider*), che altrimenti sarebbero necessari per l'acquisto delle strumentazioni informatiche ma anche per il loro mantenimento e aggiornamento. Ma la portata innovativa di questi nuovi servizi è ben visibile anche quando si pensa all'enorme quantità di dati e informazioni che vengono immagazzinati all'interno dei *database* sanitari. Le infrastrutture *cloud* consentono agli enti che le adottano, di portare all'esterno la gestione delle banche dati (in *outsourcing*), con un notevole risparmio di spesa sulla gestione. Inoltre, queste informazioni, una volta inserite all'interno di infrastrutture *cloud*, sono poste in condivisione con le altre amministrazioni sanitarie, rendendo più efficiente il sistema attraverso un accesso rapido alle stesse.

Per ragioni di "*par condicio*" è, però, doveroso specificare che l'adozione di soluzioni *cloud* è portatrice anche di criticità, che vanno affrontate affinché il trasloco verso la "nuvola" sia consapevole e responsabile.

L'elemento più immediato da considerare, in questo secondo versante, è costituito, in primo luogo, dai rischi di natura informatica, quali la perdita o il furto di dati. I *cloud server* potrebbero essere soggetti ad accessi abusivi ovvero ad azioni di danneggiamento per le più svariate finalità. Sarà, pertanto, necessario valutare ogni rischio ed adottare ogni conseguente idonea misura di sicurezza. Aspetti, questi, considerati anche a livello normativo dalla

[1] In ambito pubblico si collocano iniziative come l'informatizzazione della cartella clinica, l'introduzione del referto *on-line*, del fascicolo sanitario elettronico e del *dossier* sanitario. In una recente recensione di L. Gastaldi pubblicata nella rivista *on-line* "AgendaDigitale.eu" (http://www.agendadigitale.eu/egov/349_sette-eccellenze-di-innovazione-contro-la-malasanita.htm) sono elencati i 7 casi di eccellenza della sanità italiana che l'Osservatorio ICT in Sanità del Politecnico di Milano ha premiato perché si sono distinti per un uso efficace delle tecnologie digitali come leva di innovazione organizzativa e gestionale. Tutti gli indirizzi web citati nel presente lavoro sono stati consultati per l'ultima volta il 10 giugno 2016.

più recente disciplina Europea dettata in materia di protezione dei dati personali e anche dall'ente internazionale ISO, che nel 2014, ha pubblicato lo *standard* 27018 specificamente elaborato per i fornitori di servizi di *cloud computing*: *set* di regole finalizzate a garantire il rispetto dei principi e delle norme poste a tutela della *privacy* in chiave "*data protection by design and by default*".

Migrare l'intero comparto sanitario in *cloud* significa anche doversi destreggiare nella notevole mole normativa che lo disciplina e che deve essere combinata con le altre disposizioni complementari coinvolte nel processo di innovazione. Va tenuta certamente in considerazione la disciplina dettata in materia di protezione dei dati personali, attualmente in evoluzione, ma lo scenario diventa complicato quando i *cloud server* sono ubicati al di fuori del territorio europeo e si devono fare i conti anche con le difficoltà relative alla legge applicabile e alla competenza giurisdizionale. Non possono, peraltro, essere trascurati il Codice dell'Amministrazione Digitale (e i suoi continui aggiornamenti), la disciplina in materia di Contratti Pubblici (anch'essa recentemente abrogata e sostituita) e tutta la produzione documentale (spesso di natura provvedimentale) costituita dalle linee guida e dai manuali operativi elaborati da soggetti pubblici quali Agenzia per l'Italia Digitale e il Garante Privacy.

Proprio per tali complessità, informatiche e normative, la scelta di adottare servizi in *cloud* deve essere frutto di un'analisi articolata che tenga conto di diversi fattori. Da una parte, l'amministrazione sanitaria deve capire quanti e quali dati intende inserire all'interno della infrastruttura *cloud* e nel caso in cui i dati siano sensibili (dati sanitari, genetici, biometrici), se sceglierà una soluzione basata sul *public cloud*, è opportuno che sia valutato, con particolare diligenza, il grado affidabilità del fornitore, che deve garantire una gestione dei dati sicura e attenta. Diversa è la situazione in *private cloud*, che consente di mantenere un certo controllo sui dati inseriti e, quindi, limita i rischi generati dal conferimento dei dati ad un soggetto estraneo al titolare del trattamento.

Il Codice dell'Amministrazione Digitale, proprio in materia di sicurezza, impone particolari attenzioni per le Pubbliche Amministrazioni che organizzano i propri servizi (e dati) all'interno di una rete, come nel caso del *cloud computing*. Di particolare rilevanza, in tal senso, è l'art. 50-*bis*, il quale pre-

vede che le Amministrazioni predispongano dei piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. Il principio da seguire è quello della continuità operativa con l'obbligo di effettuare una valutazione preliminare sulle garanzie offerte dagli stessi *cloud provider*, che dovranno estendersi fino alla predisposizione di un piano di *disaster recovery*.

1.2 Obiettivi, metodologia e struttura della ricerca

Il presente lavoro è stato redatto a conclusione del XXVIII ciclo del dottorato di ricerca in "Diritto e nuove tecnologie" presso il CIRSFID[2] dell'Università di Bologna.

Le peculiarità del *curriculum* "Informatica giuridica e diritto dell'informatica" hanno orientato la ricerca verso la ricostruzione trasversale (tecnologico-giuridica) di tipo sistematico, e nel contempo funzionale, dello stato dell'arte relativo al *cloud computing* con specifico riferimento al comparto sanitario pubblico e privato.

Il contesto generale di analisi è stato quello della sanità digitale (*e-health*) e per la maggiore disponibilità di materiale bibliografico e di fattispecie da osservare, spesso si è data maggiore evidenza all'adozione del *cloud computing* nella Pubblica Amministrazione.

Il percorso d'analisi si è svolto durante le più recenti evoluzioni normative in materia di contratti pubblici e di protezione dei dati personali. Con particolare riferimento a quest'ultimo settore, l'analisi condotta considera, in parallelo, la nuova e la vecchia disciplina in quanto, per espressa disposizione del nuovo Regolamento UE 2016/679, ci si trova, attualmente, nel periodo transitorio che si concluderà il 25 maggio 2018.

L'attività di ricerca ha tenuto in debita considerazione anche le più significative pronunce delle Autorità Garanti italiane ed europee e della disciplina relativa al recente *standard* 27018 pubblicato dall'ente internazionale ISO per i *cloud providers*.

[2] Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica dell'Università di Bologna "Guido Fassò - Augusto Gaudenzi" - Dipartimento di Scienze Giuridiche.

È stata, altresì, analizzata la più recente giurisprudenza europea, che ha generato l'invalidazione dell'accordo *e Harbor* e ha condotto verso il futuro *Privacy Shield*.

Lo studio si articola in sei parti, il percorso seguito è caratterizzato dall'interdisciplinarietà tipica della tematica trattata, con tentativi di equo bilanciamento tra l'approfondimento della componente tecnologica e di quella giuridica.

Le prime due parti sono dedicate principalmente agli aspetti informatici del *cloud computing*: si parte da una ricostruzione storica per giungere alle peculiarità (e differenze) tra i modelli di servizio (*Software as a Service*, *Platform as a Service* e *Infrastructure as a Service*) e il modo in cui questi vengono distribuiti (*cloud* privato, pubblico, ibrido, comunità).

Successivamente, si passa all'analisi delle problematiche generali di sicurezza, con riferimento anche alle *best practices* proposte dalle principali organizzazioni internazionali, fino ad arrivare alle tematiche di gestione. In tale contesto non mancano precisi riferimenti alle vulnerabilità sui dati, sulle applicazioni, sulle macchine e sulle reti virtuali e alle relative conseguenze in termini di rischi per il sistema.

La parte terza, propedeutica all'esame degli aspetti giuridici del *cloud computing*, illustra la diffusione di tale tecnologia nella Pubblica Amministrazione come strumento di *e-government* e, quindi, di *e-health*. Di particolare interesse, in questa sezione, è la ricognizione dei più significativi contributi istituzionali dedicati al *cloud computing* in ambito sanitario.

La quarta parte tratta dei vantaggi e delle criticità della tecnologia *cloud* dal punto di vista giuridico, con particolare attenzione alla disciplina dettata in materia di protezione dei dati personali, anche alla luce della più recente normativa europea.

La penultima parte si sofferma sull'inquadramento negoziale dei contratti di *cloud* con sguardo rivolto alle fattispecie maggiormente diffuse nella prassi commerciale.

La sesta, e ultima, parte presenta alcune eccellenze e casi d'uso italiani, pubblici e privati, di adozione del *cloud computing* nel comparto sanitario.

PARTE PRIMA - MODELLI E ARCHITETTURE DEL *CLOUD COMPUTING*

1. Introduzione al *Cloud computing*

Ogni grande evento tecnologico che influenza i processi produttivi e, di conseguenza, le abitudini di vita dell'essere umano, ha delle implicazioni di natura giuridica. Ciò impegna il giurista nello studio delle nuove fattispecie al fine di inquadrare la disciplina ad esse applicabile.

Un settore di particolare interesse per la sua rapida e inarrestabile evoluzione è quello delle tecnologie informatiche e dei mezzi di comunicazione, caratterizzato da un mercato che propone continuamente nuovi strumenti e soluzioni sempre più sofisticate e integrate con la rete Internet, che consentono di soddisfare crescenti esigenze di informatizzazione e di comunicazione.

Da qualche anno la necessità di riorganizzazione dei flussi informativi e di razionalizzazione dei costi (sia del mondo imprenditoriale, sia della pubblica amministrazione) hanno condotto verso la diffusione di modelli eterogenei di servizio definiti genericamente *cloud computing* (o semplicemente *cloud*). Questi sono caratterizzati da un insieme di tecnologie e di modelli di servizio che favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via *web* e che promuovono, a seconda dei casi, il trasferimento dell'elaborazione o della sola conservazione dei dati dai *computer* degli utenti ai sistemi del fornitore dei servizi[1].

Il *cloud computing* non è, semplicemente, un fenomeno temporaneo o una moda, ma una vera e propria "modifica dei costumi". È la naturale evo-

[1] Nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, intitolata "*Sfruttare il potenziale del* cloud computing *in Europa*, si definisce il *cloud computing* come un modello per "*l'archiviazione, l'elaborazione e l'uso di dati su computer remoti [...] gli utenti hanno a disposizione una potenza di elaborazione quasi illimitata, non sono tenuti ad investire grandi capitali per soddisfare le proprie esigenze e possono accedere ai loro dati ovunque sia disponibile una connessione Internet*."

luzione del modo di utilizzare la Rete Internet, che da strumento per la sola condivisione documentale (la pagina *web* resa disponibile dal sito *web* remoto) diviene la porta d'accesso alle risorse elaborative di un *provider* di servizi (l'applicazione resa disponibile in modalità *web*). Le architetture *cloud* sono il frutto del potenziamento di caratteristiche già tutte insite in Internet sin dalla sua nascita, reso possibile dallo sviluppo delle tecnologie abilitanti, quali la virtualizzazione e la *software multitenancy*.

Questa trasformazione, già in atto, è maggiormente evidente nell'utenza individuale che più frequentemente, ma non sempre con completa consapevolezza anche dei possibili rischi derivanti dalle nuove tecnologie utilizzate, si avvale di servizi erogati da fornitori terzi per far fronte alle proprie esigenze informative. Si pensi, a mero titolo esemplificativo, all'utilizzo dei social network, (sui quali si trasferiscono abitualmente foto, informazioni, idee e opinioni) oppure degli strumenti di elaborazione documentale via *web* o, ancora, di *hard-disk* remoti per poter sempre disporre dei propri documenti da qualunque dispositivo e in qualunque luogo ci si trovi. Non va, peraltro, trascurata la notevole diffusione dei moderni *smartphone*, sempre connessi ad Internet, che hanno aperto la strada a innovative funzionalità, anche in ambito sociale, come, ad esempio la geolocalizzazione dell'utente. Questa ulteriore evoluzione porterà un parziale cambiamento di identità dei produttori di servizi, che saranno rappresentati dalle macchine o, meglio, dai sensori connessi ad Internet e condurrà i protagonisti della rete dal *web* partecipativo (o cosiddetto *web* 2.0) alla terza onda (*the third wave*)[2], più comunemente denominata *Internet of Thing* (*IoT*) o Internet degli Oggetti o, ancora, Internet delle Cose[3].

---

[2] Sul *cloud computing*, inteso come terza fase di internet, si veda M.R. Nelson, *Building an Open Cloud*, *Science*, 26-6-2009, 1656; di contraria opinione, considerando la nuvola una mera operazione di marketing è R. Stallman, *Cloud computing is a trap*, in theguardian.com, 29-9-2008.

[3] L. DELLO IACOVO, *Stampanti 3D, auto che si guidano da sole, intelligenza artificiale: ecco le 12 tecnologie che cambieranno il mondo*, www.ilsole24ore.it, 24-5- 2013, ove si afferma, con sguardo rivolto al futuro (2013-2025) che il *cloud computing* è una tecnologia tanto rilevante da alimentare un mercato da seimiladuecento miliardi di euro. Nel dichiarare ciò, l'Autore rinvia all'amplio studio del McKinsey Global Institute, J. Manyika et al., Disruptive technologies: Advances that will transform life, business, and the global economy, maggio 2013, in http://www.mckinsey.com/insights/business_technology/disruptive_technologies. Per la Commissione europea (comunicato 27-9-2012, IP/12/1025, Agenda digitale: una nuova

Non esiste un'unica definizione di *cloud computing* ma rappresenta certamente un buon punto di partenza quanto affermato dal *National Institute for Standards and Technology*, il quale definisce il fenomeno come "un insieme di servizi ICT accessibili *on-demand* e in modalità *self-service* tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità delle risorse e dalla misurabilità puntuale dei livelli di performance, in modo da essere consumabili in modalità *pay-per-use*"[4]. Anche l'ENISA (*European Union Agency for Network and Information Security* o Agenzia Europea sulla Sicurezza Informatica) osserva che il *cloud computing* è un nuovo modo di erogare servizi IT (e non una nuova tecnologia).

Lo studio del *cloud computing* non può essere limitato a contesti nazionali, in quanto i concetti di esternalizzazione e virtualizzazione (tipici del servizio) si accompagnano di frequente alla delocalizzazione in ambito territoriale extranazionale. Spesso, infatti, i *cloud providers* hanno la propria sede o i propri *server* in Paesi diversi da quelli fruitori dei servizi. L'Europa di questo è pienamente consapevole ed ha elaborato nel 2012 una precisa strategia per il *cloud computing* che è stata comunicata con la *EU Cloud strategy*.

Ciononostante, dal più recente (Novembre 2013) rapporto pubblicato dall'ENISA, intitolato "*Good Practice Guide for securely deploying Gover-*

---

strategia per stimolare la produttività delle imprese e della pubblica amministrazione europee attraverso "*la nuvola informatica*" - *cloud computing*, in http://europa.eu/rapid/press-release_IP-12-1025_it.htm) le iniziative previste dalla com. 2012/529 final, porteranno entro il 2020 un guadagno netto pari a due milioni e mezzo di nuovi posti di lavoro e un aumento annuo del prodotto interno lordo dell'Unione di centosessanta miliardi di euro (circa l'1%).

[4] Si veda L. BADGER, T. GRANCE, R. PATT-CORNER, J. VOAS, "*Cloud computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology - NIST* " *Special Publication* 80-146, 2012.Per la definizione di *cloud computing* si confronti, altresì, L. M. VAQUERO, L. RODERO-MERINO, J. CACERES, M. LINDNER, *ACM Computer Communication Review* , in "*A Break in the Clouds: Towards a Cloud Definition*", vol. 39, n. 1, gennaio 2009 ove si afferma che: "*I sistemi* cloud *sono grandi contenitori di risorse virtuali di facile utilizzo e accesso (che mettono a disposizione vari* software*, ma anche l'* hardware*, le piattaforme di sviluppo e/o di servizio, la potenza di calcolo). Queste infrastrutture informatiche possono essere dinamicamente riconfigurate per adattarsi a un carico di lavoro variabile (scalabilità), consentendo anche un'utilizzazione ottimale delle risorse. Questo sistema è impiegato tipicamente secondo il modello* pay-for-use *nel quale tutto è garantito dal* provider *dell'infrastruttura tramite SLA personalizzati*".

nmental Clouds"[5], si rileva che, in ambito *cloud computing*, gli Stati membri si stiano muovendo a rilento (salvo casi eccezionali) soprattutto per ragioni di tipo culturale (paure o falsi miti), piuttosto che per veri problemi di natura tecnologica.

Il rapporto dell'Agenzia Europea sulla Sicurezza informatica compie un'attenta analisi del livello di diffusione e utilizzo del *Cloud computing* nelle Pubbliche Amministrazioni di 23 Paesi membri dell'UE. L'analisi sulla strategia nazionale di *Government Cloud* dei Paesi interessati è stata condotta in duplice direzione: *cloud computing* per uso interno, da una parte e per l'erogazione di servizi all'esterno (verso il cittadino e verso le altre Amministrazioni Pubbliche).

Dalla suddetta analisi è risultato che gli Stati, nella migrazione verso il *cloud computing*, incontrano, per lo più, problemi di natura organizzativa generati da ragioni di sicurezza, di privacy e di ubicazione (quindi nazionalità) dei *data center*.

Ad oggi, risulta che, tra i Paesi membri dell'UE, soltanto Regno Unito, Spagna e Francia hanno realizzato una strategia nazionale in ambito *cloud computing*. Un altro gruppo di Stati (Irlanda, Finlandia, Slovacchia, Belgio, Grecia, Svezia e Danimarca) ha già sviluppato una strategia, che, però, non ha ancora visto attuazione concreta ma esclusivamente una progettazione e un'implementazione preliminare di servizi in modalità *cloud*. L'Italia, con l'Austria, la Slovenia, il Portogallo e la Turchia, non ha ancora una vera e propria strategia *cloud* a livello Centrale e individua l'Europa come attore principale per l'armonizzazione della disciplina dei vari Paesi. Attualmente, in questo gruppo di Stati (Italia compresa) i servizi *cloud* pubblici e delle infrastrutture sono affidati ad aziende private, generando così una frammentazione. Ciò non significa che non vi siano iniziative di ottimo livello e di valore, avviate da alcuni comparti della pubblica amministrazione Statale e Regionale, ma l'assenza di un coordinamento a livello centrale impedisce un percorso di innovazione e digitalizzazione.

Infine, esistono Paesi europei (Malta, Romania, Cipro e Polonia), fortunatamente pochi, che rimangono ancora indietro rispetto agli altri perché

[5] Il rapporto è consultabile al seguente indirizzo: https://www.enisa.europa.eu/publications /good-practice-guide-for-securely-deploying-governmental-clouds.

non solo non hanno una strategia di *cloud computing* a livello governativo ma non hanno neppure iniziative di *cloud* rilevanti.

Il report dell'ENISA, brevemente illustrato nel precedente paragrafo, contiene anche una lista di raccomandazioni sulle azioni da intraprendere per migliorare la disomogeneità attualmente presente nel contesto europeo. Si tratta, in effetti, di indicazioni già contenute (implicitamente o esplicitamente) nella strategia dell'UE del 2012.

La prima raccomandazione (*EU governmental Cloud strategy*) prende le mosse dalla constatazione che la mancanza di una strategia e di un quadro normativo sono i principali ostacoli critici per l'avvio dei servizi governativi *cloud*. Da qui si manifesta la necessità, per la buona realizzazione di un progetto di sviluppo e di implementazione del *cloud computing*, di un'azione a livello centrale (per es. dall'Unione Europea) che contenga una chiara e univoca indicazione della *governance* e dei connessi aspetti tecnici, legali e organizzativi. La *vision* e gli obbiettivi devono essere unici per tutti e, in tal senso, si auspica lo sviluppo omogeneo di servizi pubblici basati sul *cloud computing*.

Nella medesima direzione, con un'altra raccomandazione, ci si riferisce alla necessità di un quadro comune per contratti standard a livello del servizio, già dichiarata nella strategia dell'Unione Europea.

Si esprime, altresì, la necessità di sviluppo di un modello di business volto all'uso pubblico che garantisca l'efficienza e l'economia di scala dei *governmental cloud*. Questo modello consentirebbe di ridurre i costi e contemporaneamente di migliorare i servizi, in termini di affidabilità e sicurezza.

La perdita di controllo dei dati e delle risorse, infatti, è una delle principali criticità del *cloud*. In tal senso, ogni volta che una Pubblica Amministrazione mette i dati nel *cloud* deve pretendere trasparenza delle procedure adottate dal *cloud provider*. I suddetti rischi possono essere mitigati mediante l'adozione di buone clausole contrattuali sorrette, a livello normativo, da dalla recente disciplina europea[6]. Oggi può finalmente affermarsi che l'Europa sta affrontando congiuntamente tali problemi, al fine di trovare va-

[6] Regolamento del Parlamento europeo e del Consiglio n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

lide soluzioni condivise da tutti gli attori con misure che, nel contempo, incoraggiano lo sviluppo di sistemi e servizi in *cloud*.

Anche la localizzazione dei dati rappresenta un ostacolo per lo sviluppo del *cloud*. In tal senso si evidenzia l'esistenza di un quadro normativo per la posizione dei dati, che però è soltanto utile ad evitare le obiezioni da parte degli utenti governativi. In effetti, secondo l'ENISA, sarebbe molto più proficuo elaborare una disciplina comune che garantisca la sicurezza dei dati più che la loro posizione, creando un modello a cui i *cloud providers* devono adattarsi, tramite un sistema di certificazione e definendo chiaramente i requisiti di ciascun livello di sicurezza. Nell'ambito di tali prescrizioni, gli utenti pubblici e i fornitori dovrebbero essere liberi di scegliere il livello di sicurezza previsto e richiesto per i servizi pubblici, dopo una valutazione del rischio che dovrebbe essere effettuata prima dell'avvio dei progetti. Infine, tra le raccomandazioni, si parla anche di protezione dei dati personali, con espresso riferimento all'accesso autenticato e alla crittografia, che nel *cloud* non hanno trovato una implementazione matura.

1.1 Cenni storici

Il *cloud computing* ha subito un'evoluzione che è passata attraverso diverse fasi storiche. È stato un percorso articolato partito dal *grid computing* dei primi anni novanta, in cui si teorizzava attraverso il concetto di "griglia" la possibilità di sfruttare all'occorrenza risorse e potenze computazionali geograficamente distribuite, similmente a quanto accade nella rete elettrica con la produzione, la trasmissione e la distribuzione dell'elettricità all'utente finale su richiesta[7]. Si è giunti, infine, all'A*pplication Service Provider* di fine anni novanta, un modello di business in outsourcing in cui venivano messe a disposizione applicazioni *software* acquistate dal cliente, ospitate e gestite nei *data center* centralizzati del *provider*, attraverso infrastrutture dedicate per loro. In breve ogni cliente aveva in uso la propria istanza di un'applicazione, accessibile tramite una connessione Internet o rete privata,

[7] I. FOSTER,C. KESSELMAN, The Grid: Blueprint for a New *Computing* Infrastructure, San Francisco, Morgan Kaufmann, 1999.

su *server* dedicato[8]. Ma l'idea di poter sfruttare e utilizzare risorse computazionali attraverso una rete globale risale già agli anni '60.

Nel 1961 il professore J. McCarthy, durante le celebrazioni del centenario del MIT, osservava, nel trattare il *computing* come una pubblica utilità: "*Each subscriber needs to pay only for the capacity he actually uses, but he has access to all programming languages characteristic of a very large system […]. Certain subscribers might offer service to other subscribers […]. The computer utility could become the basis of a new and important industry*"[9].

Nel 1963 J.C.R. Licklider, già responsabile del progetto ARPANET[10], propose l'idea di un *Intergalactic Computer Network* in un *memorandum*[11] inviato ai suoi colleghi, nel quale ipotizzava che chiunque, in un futuro prossimo, avrebbe potuto sfruttare una rete interconnessa di *computer* con la possibilità di accedere a programmi e dati da qualsiasi *site*.

Una delle prime compagnie "*dot-com*" a introdurre il concetto di applicazioni aziendali distribuite tramite il proprio sito *web*, accostandosi, per certi aspetti, all'idea primitiva del *cloud computing*, è stata "Salesforce.com", nel 1999.

Un ulteriore sviluppo, a partire dal 2002, ha portato Amazon con i suoi *Amazon Web Services* (*AWS*)[12], fornendo una serie di servizi "*cloud-based"* che hanno permesso agli sviluppatori di non dover dipendere da un propria infrastruttura di *Information Technology* (IT). Tra i principali AWS si può citare il lancio nel 2005 di *Amazon Mechanical Turk* (*MTurk*)[13], un servizio Internet di tipo collaborativo, con interfaccia programmabile, che permette agli sviluppatori, i *Requester*, di risolvere quesiti che non possono essere affidati a un *computer* e necessitano dell'intervento umano dei *Workers* iscritti

---

[8] C. BENNET, G. T TIMBRELL, *Application Service Providers: Will They Succeed?*, in Information Systems Frontiers (ISF), vol. 2, n. 2, 2000, pp. 195-211.

[9] S. GARFINKEL, *The Cloud Imperative*, in "*MIT Technology Review*", (2011), http://www.technologyreview.com/news/425623/the-*cloud*-imperative/

[10] G. DONALD, *Arpanet*, in Wikipedia (2014), http://en.wikipedia.org/wiki/ARPANET.

[11] J.C.R. LICKLIDER, *Memorandum For Members and Affiliates of the Intergalactic Computer Network*, http://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-*computer*-network

[12] *Amazon Web Services*http://aws.amazon.com.

[13]*Amazon Mechanical Turk*, in "Wikipedia", (2013), http://it.wikipedia.org/wiki/Amazon_Mechanical_Turk

alla *community*. Questi ultimi, tutti assieme, coordinano intelligenze umane nelle loro applicazioni. Nel 2006 ha luogo la presentazione dell'AWS *Elastic Compute Cloud* (EC2)[14]. È un servizio *web* che offre al cliente un ambiente di elaborazione virtuale che permette varie operazioniquali l'installazione di un ambiente applicativo, la gestione delle autorizzazioni di accesso alla rete e l'esecuzione di programmi, il tutto con un facile accesso all'infrastruttura di calcolo privata di Amazon. Nello stesso anno annuncia l'offerta di *AWS* S3[15]. Questo servizio, al contrario di EC2 che mette a disposizione risorse computazionali nel *cloud*, fornisce capacità di memorizzazione, tramite una semplice interfaccia *web*, per archiviare e recuperare una qualsiasi quantità di dati da qualunque luogo sul *web*.

Un importante contributo, per il *cloud computing*, è derivato dall'emergere di "*killer application*"[16]. Un esempio lo forniscono alcuni servizi Microsoft e Google, affidabili, di facile uso e con una grande diffusione nel mercato odierno, con l'effetto di una generale accettazione da parte dell'utente finale. Già nel 2006 Google ha iniziato ad offrire applicazioni aziendali basate su *browser*, completando sempre più la suite dei servizi *Google Apps*[17]. Nel 2008 ha rilasciato *Google App Engine* (GAE)[18], una piattaforma *cloud* messa a disposizione per gli sviluppatori che intendono creare applicazioni *web* senza dover gestire in prima persona l'infrastruttura necessaria, è unicamente necessario fornire il codice sorgente. Microsoft con il suo *Windows Azure*[19], rilasciato nel 2008, utilizza *Windows Azure Hypervisor* (WAH) come infrastruttura *cloud* con virtualizzazione dei servizi, per offrire all'utente sia sviluppo sia servizi di archiviazione e integrazione delle proprie applicazioni.

---

[14] *Amazon Elastic Compute Cloud*, in "Wikipedia" (2013), http://it.wikipedia.org/wiki/ Amazon_Elastic_Compute_*Cloud*

[15] *Amazon S3*, in "Wikipedia", (2013), http://it.wikipedia.org/wiki/Amazon_S3

[16] La *killer application* (letteralmente "applicazione assassina") è un'espressione riferita ad un prodotto *software* di successo. Questi *softwares* sono basati su una tecnologia che penetra nel mercato, imponendosi rispetto alle tecnologie concorrenti, aprendo così la strada alla commercializzazione di altre applicazioni secondarie. *Killer application*, in "Wikipedia", (pagina modificata il 15 set 2014), http://it.wikipedia.org/wiki/Killer_application

[17] *Google Apps*, http://www.google.com/enterprise/apps/business/

[18] *Google App Engine*, https://cloud.google.com/appengine.

[19] *Microsoft Azure*, in "What is Windows Azure?", (2013), http://www.windowsazure.com/en-us/documentation/?fb=it-it

Al momento il termine *cloud computing* è diventato d'uso comune e, oltre a questi esempi di servizi *cloud* pubblici, diverse realtà aziendali hanno sperimentato e realizzato sistemi interni e quindi privati. Il *cloud computing* è oramai una strategia chiave per gli IT. La figura 1 mostra la popolarità di questo termine rispetto a *grid computing* e *virtualization*, in termini di interesse di ricerca di queste parole chiave sul motore di ricerca Google.

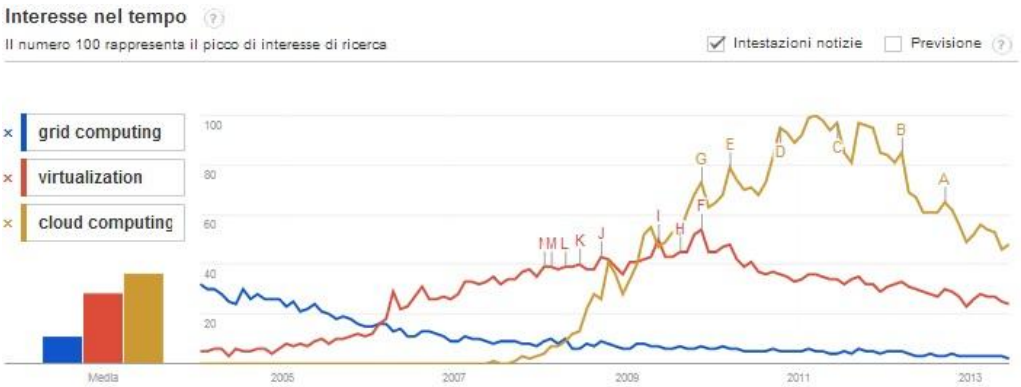

Figura 1: Popolarità nelle ricerche *web* ricavate da Google Trends[20]

1.2 Caratteristiche

Ci sono diverse caratteristiche che contraddistinguono un ambiente di *cloud computing*. Dal punto di vista di colui che accede, singolo utente o azienda, vi è un'ampia offerta che riduce al minimo i costi del servizio. Ad esempio l'infrastruttura utilizzata per fornire il servizio può essere di proprietà del *Cloud Provider* e i suoi utenti non sono vincolati all'uso di uno specifico dispositivo d'accesso connesso ad Internet né alla loro posizione geografica[21].

Le reti convenzionali per *data center* sono studiate per utilizzare piattaforme tradizionali che, per loro natura, sono statiche, poco flessibili e incapaci di scalare e soddisfare le esigenze dinamiche di un *cloud data center* che implementa virtualizzazione e mobilità delle applicazioni, dei servizi e dei processi computazionali. L'architettura della rete informatica necessita

[20] Fonte: https://www.google.it/trends/

[21] G. ZHAO, J. LIUJ, Y. TANG, W. SUN, F. ZHANG, X. YE, N. TANG, *Cloud Computing: A Statistics Aspect of Users*, In First International Conference on *CloudComputing* (*Cloud*Com), Beijing, China, Heidelberg Springer Berlin, (2009), pp. 347–358.

di essere ridisegnata e semplificata. Un'architettura tradizionale non sarà in grado si supportare con successo il *cloud computing*, per questo dovrà essere più agile per soddisfare le aspettative degli utenti. Per esempio un servizio di *hosting* per *upload* di *file* e gestione del contenuto può rispondere velocemente e in tempo reale alla richiesta di modifica *file*, ma sarà meno reattivo nel caso si richieda al *provider* un adeguamento della potenza di calcolo o l'introduzione di un *database* nel sistema.

Gli ambienti *data center* tradizionali sono progettati con uno specifico fabbisogno di energia di alimentazione in termini di kW/rack. Negli ultimi anni si è assistito ad una sempre più crescente richiesta di prestazioni che ha fatto aumentare il numero dei *server* e i consumi, con il conseguente aumento della capacità di raffreddamento del sito. Ciò comporta la limitazione del numero di *rack* che un *data center* può supportare, pur avendo ancora dello spazio fisico a disposizione per la sua espansione.

Il *cloud* offre flessibilità, rispetto ai tradizionali *data center*, perché, sfruttando le tecnologie di virtualizzazione, consente di fare un rapido *provisioning* di un nuovo *server* o il *deployment* di un'applicazione o di specificare la potenza di calcolo per un determinato *service* richiesto dall'utente. La conseguenza diretta è l'abbassamento dei costi perché non sarà necessario per l'azienda cliente investire patrimonio aziendale per ottenere gli stessi servizi con un proprio *data center*, dotato di una solida infrastruttura affidabile in termini di prestazioni e sicurezza delle informazioni. Sarà, per esempio, sufficiente connettersi al *cloud* invece di installare il *software* da eseguire sul proprio *hardware*. Per molti utenti il *cloud* appare, infatti, come un singolo punto di accesso alla nuvola, accessibile da Internet con un semplice *web browser*. In realtà diverse infrastrutture *cloud* distribuiscono i servizi attraverso una rete di *data center* condivisi, sia fisici che virtuali. Per alcuni di questi servizi non è prioritario prestare attenzione a dove i dati siano fisicamente localizzati o dove lo siano i *server*. L'importante è usufruirne all'occorrenza e in tempo reale[22].

[22] F. BAZARGAN, C. Y. YEUN, M. J. ZEMERLY, *State-of-the-Art of Virtualization, its Security Threats and Deployment Models*, in International Journal for Information Security Research (IJISR), vol. 2, (2012), pp. 335-336

Il modello di *cloud computing* si basa su cinque caratteristiche chiave, rispetto agli approcci tradizionali, così come definito nella *Security Guidance*[23] a cura della *Cloud Security Alliance*:

-Servizio *self service* su richiesta. Attraverso un portale sicuro l'utente di servizi *cloud* seleziona e modifica le proprie risorse IT (servizi per *server*, rete e *storage*) quando è necessario, senza intermediazione con il *provider* di *cloud*. In questo modo l'utente ha pieno controllo sui servizi che consuma. L'interfaccia *self-service* deve essere *"user-friendly"* e deve offrire facilità di gestione. Un altro aspetto positivo é l'eliminazione dell'interazione umana con il *provider* che comporta efficienza e risparmio.

-Ampio accesso alla rete. L'accesso ai servizi *cloud* deve essere universale, ovvero si deve poter accedere tramite dispositivi standard ed eterogenei tra loro sia fissi che mobili, quali telefoni, *laptop*, PDA[24] ecc. Deve essere altresì garantita l'integrità dei dati e l'autenticazione.

-Condivisione delle risorse. Le risorse computazionali messe a disposizione dal provider vengono raggruppate per servire tutti gli utenti con diverse risorse fisiche e virtuali, assegnate dinamicamente e riassegnate in base alla domanda. Dal punto di vista dell'applicazione dove e con quali risorse fisiche questi dati siano elaborati, trasmessi e memorizzati, non ha importanza, non è necessario alcun controllo o conoscenza circa la posizione esatta delle risorse richieste. Questo grado di astrazione è generalmente raggiunto per mezzo di virtualizzazione a livello di *chipset* e di sistema operativo o abilitata ai livelli più alti con *file system* e protocolli di comunicazione personalizzati.

-Scalabilità ed elasticità. Il *cloud computing* utilizza le tecnologie Internet per offrire funzionalità IT o *service* che siano altamente scalabili. Un'applicazione *cloud* che sia scalabile, ovvero che non manifesti alcuna caduta di prestazione all'aumentare del numero di utenti, coinvolge tre meccanismi: la posizione o mobilità (i servizi possono risiedere ovunque e su qualsiasi dispositivo e possono essere invocati da qualsiasi posizione); la replica dei dati (per offrire ridondanza e garantire *business continuity* e *disa-*

[23] CSA, *Security guidance for critical areas of focus in cloud computing*, 2011 3°, (2009), p. 28.
[24] PDA = *Personal Digital Assistant*

ster recovery[25]); il bilanciamento del carico (consente di ottimizzare l'uso di un'istanza di una risorsa *cloud* per soddisfare al meglio la domanda). Se la domanda cresce allora verranno messe a disposizione nuove istanze e aggiunte al servizio, così da assicurarne il mantenimento elevato in termini di prestazioni. Se poi questo processo è anche capace di rispondere efficacemente ad una contrazione della richiesta, eliminando le istanze preposte, allora lo definiamo un sistema "elastico".

-Servizio controllato. I servizi *cloud* usano un modello di pagamento *pay-per-use*[26] basato sull'ottimizzazione dell'uso e consumo delle risorse e della loro allocazione dinamica (possono risiedere su *hardware* virtualizzato in molteplici locazioni), fornendo metodi per la loro gestione e misurazione, sia lato cliente che *provider*. Questo si traduce in una maggiore efficacia nella previsione dei costi associati. La combinazione tra astrazione e servizi fatturati per quanto effettivamente venga usato, rappresenta una separazione tra i requisiti architetturali di un sistema *cloud* e uno tradizionale.

Oltre alle caratteristiche fin qui esaminate, anche il design della LAN di un *data center* in ambente *cloud* merita un approfondimento, alla luce delle molteplici revisioni subite nel corso degli ultimi decenni, evolvendosi da una singola posizione di elaborazione e archiviazione ad una architettura distribuita *client-server*, sino al *data center* virtualizzato.

A partire dagli anni novanta gli *switch* Ethernet entrarono nella progettazione di una generica rete locale. Il *design* del sistema prevedeva in genere una struttura gerarchica a tre livelli, che serviva a compensare i limiti delle prestazioni di *switching* e che si adattava ad una architettura *client-server* tipica del periodo storico. Questo principio costruttivo multi livello fu impiegato anche all'interno dei *data center* ed è stato testato e migliorato nel corso degli anni, tanto da essere diffusamente impiegato tuttora nell'attuale generazione[27].

La figura 2 mostra un possibile esempio di questo design: un primo livello definito "*access*" che collega fisicamente tutti i dispositivi *server* alla rete tramite *switch* di accesso di livello 2 OSI (a sinistra) e *link* da 1 Gbps

[25] Capacità aziendale di mantenere la continuità operativa a seguito di evento dannoso e predisposizione delle misure atte al ripristino dei sistemi in caso di emergenza.

[26] Il servizio viene concepito come un'utility: pago per usarlo.

[27] D. BARNES, B. SAKANDAR, *Cisco LAN Switching Fundamentals*, Ciscopress, 2005, pp. 287-289

principali e di *backup*, ed eventualmente di livello 3 (a destra), per coprire eventuali esigenze di piccoli domini di *broadcast* L3 e isolamento di *server*. Ciascun *switch* d'accesso è di solito collegato a due *switch* di livello intermedio o di aggregazione, per la ridondanza, con *link* da 10 Gbit/s. Questo livello è normalmente costituito da *switch* L3 per il *routing* tra i domini della rete. Gli *switch* L3 segnano il confine tra un dominio di livello 2 OSI e uno di livello 3, sono impegnati nell'analisi dei flussi di traffico che attraversano il *data center*, in servizi di dominio, di bilanciamento del carico tra *server* e nei controlli di *firewalling* e *intrusion detection*.

Il livello superiore definito di *core* fornisce connettività ridondante a *switch* multipli di livello aggregazione, con compiti di smistamento ad alta velocità del traffico, per tutti i flussi che entrano ed escono dal *data center*. Tipicamente il traffico di rete associato ad una tradizionale applicazione *client-server*, viaggia su e giù tra i livelli dell'architettura, con il *server* posizionato nel *design* all'interno di un piccolo blocco di livello 2 detto POD (flusso definito Nord-Sud), tramite nodi e *link* ridondanti, creando, come si evince dallo schema in figura 2, dei *loop* fisici che risulterebbero dannosi all'interno di un dominio L2 (traffico che entra nel circolo senza mai raggiungere una destinazione)[28].

[28] Un dominio L3 con protocollo IP implementa la *feature* del TTL per eliminare un pacchetto arrivato al suo limite di vita (TTL = 0)

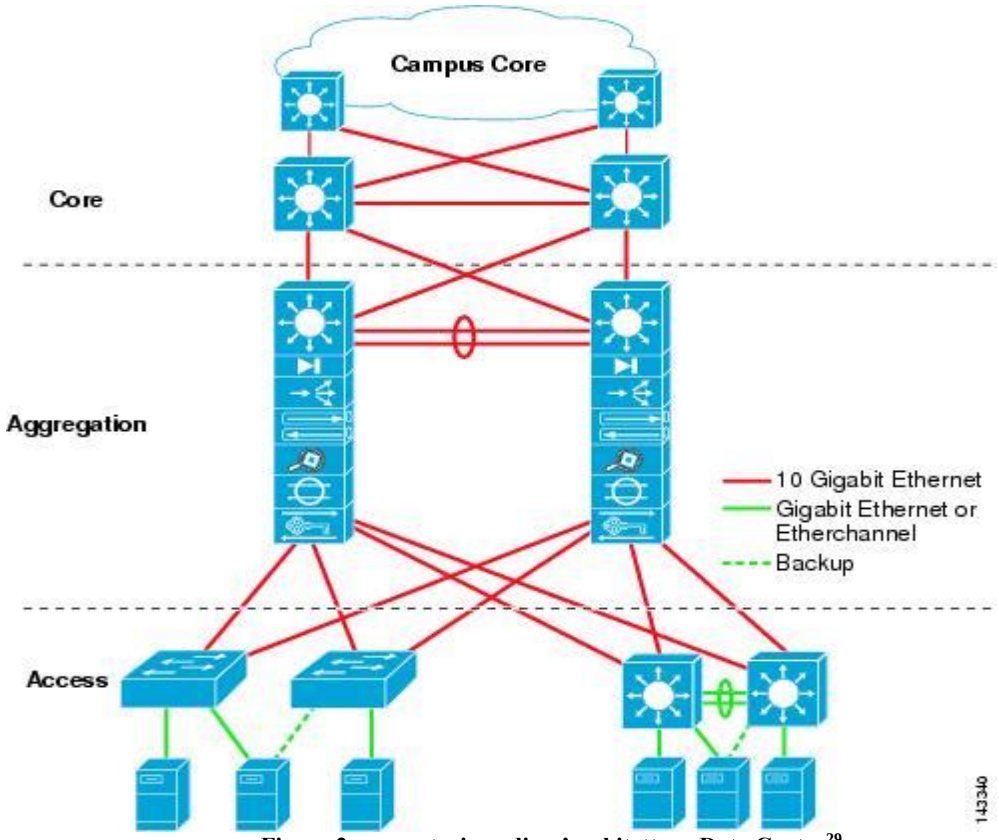

Figura 2: presentazione di un'architettura Data Center[29]

Per risolvere il *loop* a livello logico, mantenendo le connessioni fisiche, si può ricorrere a *Spanning Tree Protocol* (STP) [30] che calcola e vede la rete come un albero logico dove tutti i nodi (*switch*) sono interconnessi senza *loop* a partire da uno *switch* radice, creando un unico percorso attivo tra due nodi e disattivando i *link* che non fanno parte dello *spanning tree*. I *link* bloccati diventeranno attivi solo quando qualcuno tra quelli attualmente attivi fallirà. La limitazione di STP nel non usare tutti i *link* disponibili per evitare i *loop* e il fatto che non abbia tempi ridotti di risposta ai *link failure* e conseguente ripristino dalla condizione d'errore, ha permesso di sviluppare delle alternative.

Tra queste è bene citare *virtual PortChannel* (vPC)[31] di Cisco, si veda la figura 3, che abbina i benefici della ridondanza tra switch diversi a quelli

[29] Fonte: cisco.com

[30] K. SOLIE, L. LYNCH, *CCIE Practical Studies*, vol. II, Ciscopress, 2004, pp. 28-35

[31] Cisco Systems, *Virtual Port Channel Quick Start Guide*, in "Cisco Nexus 3000 Series Switches",

dell'aggregazione di link fisici tra loro. In tal caso accadrà che l'unione tra link appaia come un unico link logico, vedi figura 3, che resterà attivo nello *spanning tree* finché almeno un link membro del gruppo sarà disponibile, eliminando così la dipendenza dalle porte bloccate STP, come indicato in figura 4.

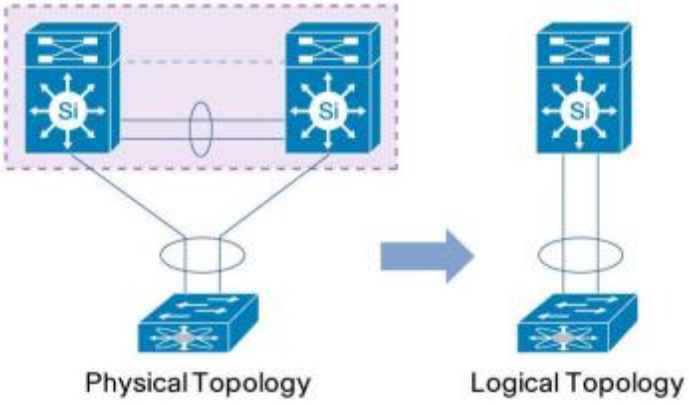

Figura 3: Creazione di un singolo nodo logico in tecnologia vPC[32]

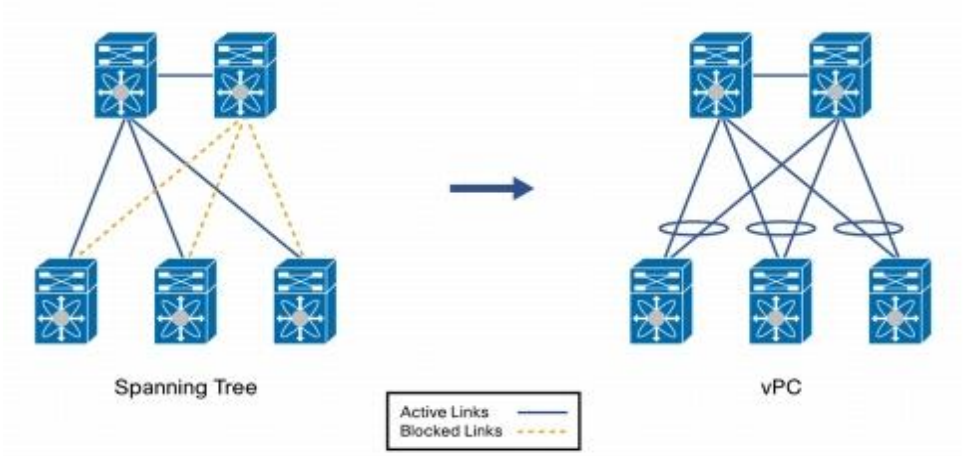

Figura 4: vPC comparato a STP[33]

L'approccio Nord-Sud è basato su pattern di traffico oramai obsoleti e i modelli di sicurezza non si adattano alle esigenze attuali di *cloud computing*, con utenti diversi che richiedono differenti livelli di servizio. Il tutto si tra-

---

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps11541/white_paper_c11-685753.html

[32] Fonte: Cisco.com

[33] Fonte: Cisco.com

duce in inefficienza unitamente a una complessità di rete non necessaria e poco scalabile e ad alti costi.

Invece la nuova generazione dei *data center*, che fa largo uso delle tecnologie di virtualizzazione, genera una significativa quantità di traffico *server-server* (definito per questo Est-Ovest), interna al *data center*, con un livello di rete costituito da *switch* virtualizzati e il flusso che si sposta tra *server* virtuali che condividono un *pool* di risorse, magari attestate su macchine fisiche diverse, su diversi POD o diversi *data center* geografici, con una estensione del dominio L2 per consentire la migrazione di macchine virtuali tra loro[34]. Anche una recente previsione di Cisco[35], mostrata in figura 5, conferma la tendenza, sul periodo 2011-2016, che il traffico interno al data center rappresenta la maggioranza rispetto a quello che lo attraversa, per motivi quali la separazione per funzioni dei *server* di applicazioni e per attività

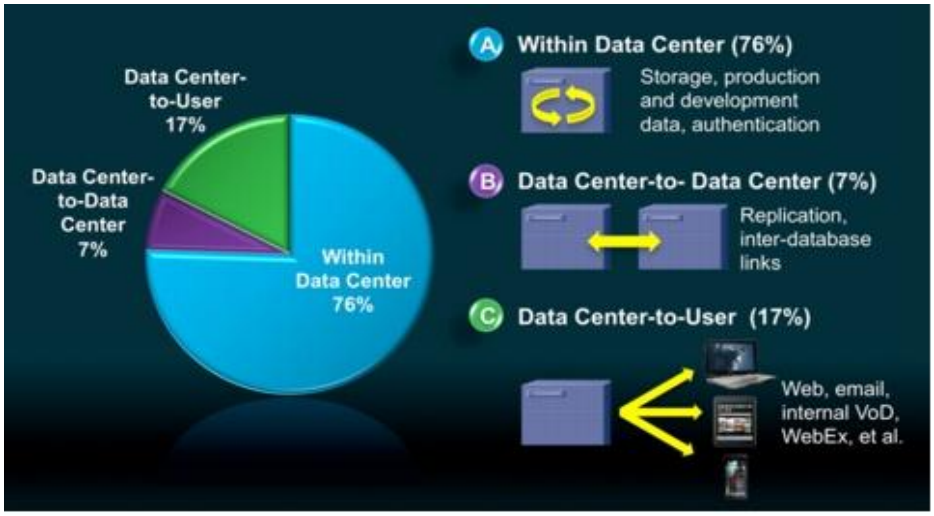

Figura 5: traffico globale Data Center per destinazione[36]

di replica e backup.

L'architettura a tre livelli non è stata progettata per gestire il traffico "*server-server*" senza dover andare avanti e indietro attraverso i livelli, sarebbe inefficiente e si avrebbe l'aggiunta di latenza ad ogni hop. Questo mal

[34] Brocade, *Brocade One Data Center-Cloud-Optimized Networks*, in "Position Paper" (2011), http://docs.media.bitpipe.com/io_10x/io_102560/item_479611/CloudOptimizedNetworks_GA-PP-350.pdf

[35] Cisco Systems, *Cisco Global Cloud Index: Forecast and Methodology, 2011–2016*, in Global *Cloud* Index (CGI), (2012)

[36] Fonte: Cisco.com

si adatta, per esempio, ad applicazioni *real time (unified communications*)[37] tipiche di scenari *cloud computing*.

Il nuovo approccio prevede una gerarchia piatta a due livelli, con il livello accesso e i due livelli *aggregation* e *core* condensati in uno solo, quindi meno hop da attraversare e minore numero di porte e connessioni[38]. Per garantire un'alta disponibilità di risorse, il *data center* di ultima generazione, dovrebbe ampliare, come detto in precedenza, la dimensione del dominio di livello 2, così da consentire in maniera trasparente lo spostamento di dispositivi e la modifica dell'infrastruttura. Questo, tuttavia, comporterebbe dei problemi legati allo *spanning tree*, che non consente di scalare con flessibilità quanto invece sarebbe permesso una tecnologia di livello 3. Servirebbe un compromesso tra la flessibilità fornita dal livello 2 e la scalabilità del livello 3.

Cisco *FabricPath*[39] rappresenta un'alternativa a STP e vPC, mantiene tutti i *link* attivi ed è più facile da implementare rispetto a vPC. *Switch* multipli configurati con *Fabricpath* partecipano alla stessa topologia, vengono visti e operano come se fosse un unico grande *switch* virtuale, quindi consentono di estendere una particolare VLAN, con il risultato di abbassare la complessità ed aumentare il dominio senza i problemi STP.

Nella figura 6 vediamo come un classico *frame Ethernet* che si presenta in ingresso sullo *switch* di bordo della *fabric* (porta di *edge*), viene incapsulato con un *header* che presenta indirizzi instradabili, *switch* sorgente e *switch* destinazione, e viene inoltrato su altri *switch* lungo un percorso di porte *core*. All'uscita dalla *fabric* ci sarà il de incapsulamento e la consegna.

Gli *switch* di accesso possono raggiungersi a vicenda a livello 2, consentendo in tal modo uno spostamento delle macchine virtuali in pochi istanti. Non essendo necessario che un *server* si trovi fisicamente in un POD speci-

---

[37] *Unified Communications*, in "Wikipedia", (2013), http://en.wikipedia.org/wiki/Unified_communications

[38] S. R. SMOOT, N. K. TAN, *Private Cloud Computing*, Morgan Kaufmann, 2012, p. 44

[39] CISCO SYSTEMS, Sc*ale Data Centers with Cisco FabricPath*, in "Cisco Nexus 7000 Series Switches", http:http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/white_paper_c11-605488.html

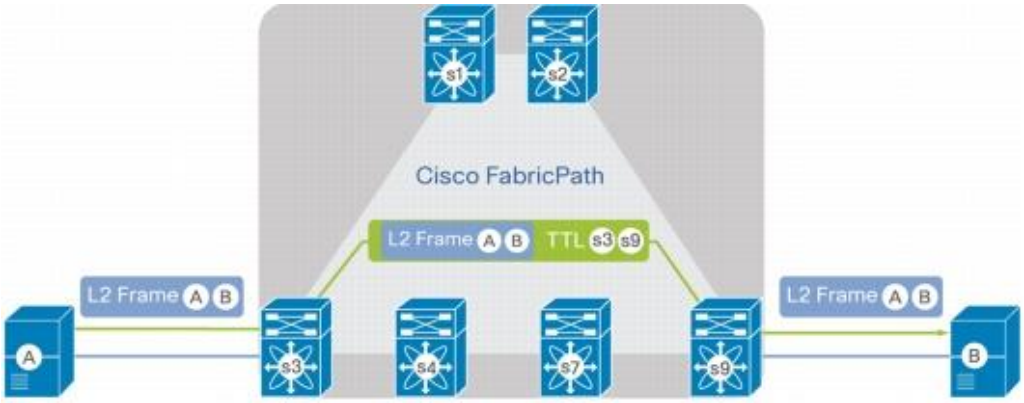

Figura 6: Trasporto di frame utilizzando Cisco FabricPath[40]

fico, si facilita il *provisioning* dinamico. Fa uso di un protocollo di *routing* quale IS-IS per operare lo scambio di informazioni riguardanti i vari indirizzi MAC *address* e calcolare il *best path* verso la destinazione. Quindi si tratta di un *routing* di livello 2, con la possibilità di sfruttare in parallelo la totalità dei collegamenti presenti, sino ad un massimo di 16 percorsi *Fabric path* e ciascuno di questi può essere il frutto di un'aggregazione *PortChannel* da 16 porte (per fornire una maggiore larghezza di banda, ridondanza e bilanciamento del carico), per un totale di 256 *link* attivi.

1.3 Astrazione e ottimizzazione delle risorse fisiche attraverso la virtualizzazione di sistemi, *network* e *storage*

Uno dei principali fattori che hanno portato a rivalutare gli scenari originali in ambito data center è la virtualizzazione. Essa rappresenta l'astrazione di risorse fisiche in entità logiche, tale che una singola risorsa fisica possa apparire come un numero di entità logiche (virtualizzazione uno-a-molti) e le molteplici risorse fisiche possano rappresentare una singola entità logica (virtualizzazione molti-a-uno). Questa astrazione nasconde le caratteristiche fisiche e i dettagli irrilevanti di queste risorse: ogni utente ottiene l'illusione di esserne l'unico utilizzatore. Quindi la virtualizzazione può essere applica-

[40] Fonte: Cisco.com

ta a diverse aree IT, come ad esempio: *server*, *desktop*, *storage*, *network*, applicazioni, servizi e altro ancora[41].

L'introduzione delle tecnologie di virtualizzazione all'interno dei data center, da prima sui *server*, è stata infatti sin da subito un punto di forza per il *cloud computing*, perché abbassa i costi di replica e di mobilità della domanda di risorse. Un nuovo modo per consumare risorse *software*, di calcolo, di memorizzazione e di rete, offrendo un modello di pagamento a consumo.

Nella virtualizzazione di un *server* il *software* chiamato *hypervisor*, consente a più macchine virtuali (VM), impostate con CPU, RAM *networking*, spazio disco, sistema operativo e applicazioni, la loro esecuzione sullo stesso *server* fisico, come illustrato nella Figura 7.

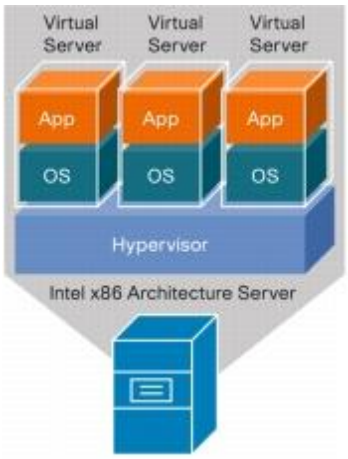

Figura 7: Architettura di virtualizzazione *server*[42]

La configurazione può anche portare ogni macchina virtuale ad emulare un *computer* fisico creando un ambiente di sistema operativo separato, così che sia isolata e non a conoscenza delle altre. Per permettere di eseguire più macchine virtuali contemporaneamente sullo stesso *server*, *l'hypervisor* dinamicamente separa e condivide le risorse fisiche disponibili sull'*host*, come ad esempio: CPU, memoria e dispositivi di I/O. Le funzionalità dell'*hypervisor* variano a seconda del *vendor* (VMware, Microsoft, Citrix e altri) e in base all'architettura e all'implementazione.

[41] A. J. YOUNGE, R. HENSCHEL, J. T. BROWN, G. VON LASZEWSKI, J. QIU, G. C. FOX, *Analysis of Virtualization Technologies for High Performance Computing Environments*, in Aa.Vv., IEEE 4th International Conference on *Cloud Computing*, (2011)

[42] Fonte: Cisco.com

La virtualizzazione, inoltre, consente il consolidamento dell'*hardware* lato *server*, ovvero permette di sfruttare al meglio le risorse fisiche del *server* non lasciando che, come accade di frequente, sia sotto utilizzato a causa di un unico *workload*[43]. Mentre invece il *deploy* di centinaia di VM su un *server* può giustificare i costi di energia, di raffreddamento, dell'infrastruttura di rete e di gestione dello stesso, poiché ogni VM rappresenta un sistema completo, rendendo quindi possibili *workload* multipli sulla stessa macchina fisica e quindi ottimizzandone l'utilizzo[44].

Applicando il concetto di scalabilità alla virtualizzazione, questa si traduce nell'essere in grado di fare un *deployment* veloce di nuove macchine virtuali su un *server* fisico esistente e poi di eliminarle quando non sono più necessarie. Non solo, anche scalabilità in termini di aggiunta o rimozione di CPU, RAM e spazio disco virtuali, oppure l'aggiunta di funzionalità abilitando *software* aggiuntivo o nuove istanze, in quanto, se ciò che stato aggiunto non dovesse più essere richiesto, basterà di nuovo eliminare le istanze. Più in generale si viene a creare una piattaforma *cloud* scalabile che in maniera trasparente ospita le risorse disponibili all'aumentare delle esigenze applicative o che in qualsiasi momento può avere una grande variabilità nel numero di utenti, senza la necessità di dover subire il picco di carico.

I concetti di virtualizzazione possono essere applicati anche a livello *network* attraverso la segmentazione di una rete fisica in molteplici reti virtuali o nell'inglobazione di molteplici reti fisiche in una rete virtuale. Questo è stato reso possibile a partire dall'implementazione dello *switch* virtuale (o semplicemente vSwitch) all'inizio degli anni 2000 a cura di VMware, che ha introdotto un nuovo campo del *networking* con l'obiettivo di gestire il traffico delle macchine virtuali controllate da un *hypervisor*. Un esempio di *switch* virtuale quale il Nexus 1000V di Cisco non implementa il protocollo *Spanning Tree*.

Infine, la virtualizzazione a livello *storage*, o unità di memorizzazione, combina molteplici dispositivi di archiviazione fisici in dispositivi logici. Si può definire come "*storage* a blocchi" l'astrazione di uno *storage* fisico che

[43] *Workload* = quantità di elaborazione che impegna un *server* ad eseguire un'applicazione e a supportare un numero di utenti che interagiscono con essa

[44] Q. ZHANG, L. CHENG, R. BOUTABA, *Cloud computing: state-of-the-art and research challenges*, in J Internet Serv Appl (2010), p. 9

può essere utilizzato come risorsa di memorizzazione indipendentemente dalla sua posizione fisica o struttura. L'accesso ai dati avviene per interi blocchi di informazione e questo sistema è tipico delle reti S*torage Area Network (*SAN). Oppure come "*storage a file*" che definisce l'astrazione per i dati accessibili a livello di *file* e non di blocco, dalla posizione fisica nella quale sono memorizzati, su un *file system* definito *Network Attached Storage (NAS).*[45]

1.4 Infrastrutture *multi-tenancy* per l'implementazione condivisa di soluzioni applicative

Tradizionalmente una rete aziendale ha il proprio *server* privato e dedicato che offre istanze dedicate del *software*. Queste applicazioni si definiscono *single-tenant*. I provider *cloud* offrono i servizi applicativi ai propri clienti tramite un'infrastruttura condivisa delle applicazioni, progettata per essere *multi-tenant*, che ne promuove l'uso concorrente tra un numero elevato di utenti, virtualmente segmentando i dati e la configurazione in modo che ogni utente lavori con un'istanza virtuale e personalizzata dell'applicazione richiesta. Il *multi-tenancy* si esprime in modi diversi nei diversi modelli di servizio del *cloud*, in figura 8 alcuni esempi.

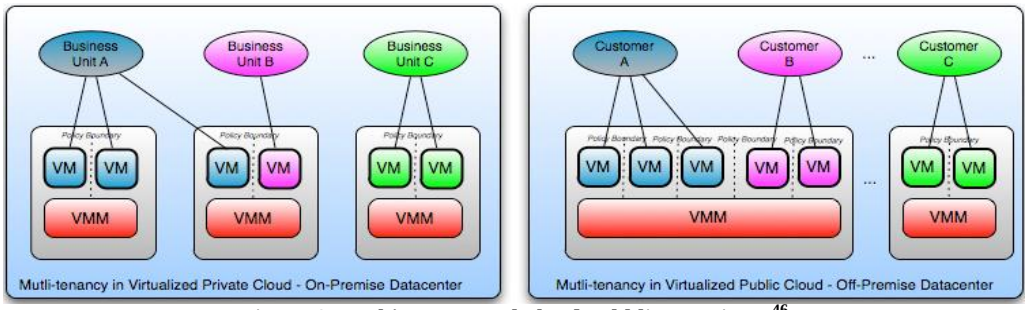

Figura 8: *Multi-tenancy* nel *cloud* pubblico e privato[46]

Non solo molteplici *tenant* possono condividere la stessa applicazione, ma diverse macchine virtuali, tramite il loro *hypervisor*, condividono l'hardware e diversi processi condividono lo stesso sistema operativo e/o

[45] C. P. CONDE, W. D. VILLANUEVA, *Virtualization as a support for SOA and cloud computing*, in Aa.Vv. *Monograph: 2010 – Emerging Information Technologies (II)*, "The European Journal for the Informatics Professional" vol. XI, 2010, pp. 5-6

[46] Fonte: *Cloud Security Alliance*

servizi di rete. Questo rappresenta una delle ragioni per i vantaggi economici del *cloud computing*[47].

1.5 Architettura del *Cloud computing*

Secondo il già citato *Cisco Global Cloud Index* (GCI)[48], che fornisce previsioni sulla crescita, e i trend del traffico IP globale che coinvolgono i data center ed il *cloud* in un arco temporale che va dal 2011 al 2016, l'offerta di servizi di *cloud* è in rapida ascesa. In generale si prevede che il traffico globale dei data center quadruplicherà e, in particolare, il traffico IP del *cloud* aumenterà di sei volte entro il 2016, raggiungendo 4,3 *zettabyte*[49].

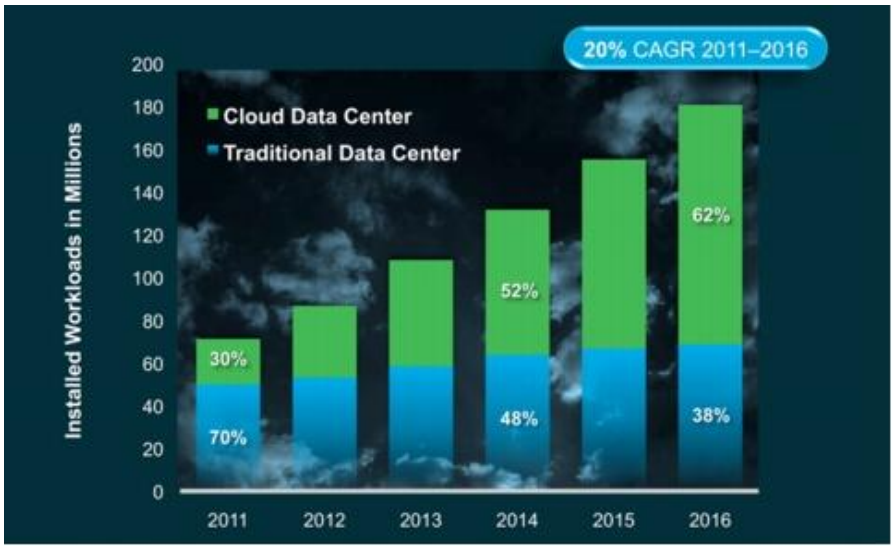

Figura 9: Workload Distribution: 2011-2016[50]

Analizzando la figura 9, che mostra l'evoluzione del traffico da un data center tradizionale a uno di tipo *cloud* in termini di *workload*, entro il 2016quasi i 2/3 di *workload* totali saranno processati in *cloud data center* con un tasso totale di crescita annuale composto (CAGR)[51] del 20% e la cre-

[47] G. SCHULZ, *Cloud and Virtual Data Storage Networking*, CRC Press, 2012, p. 56

[48] Cisco Systems, *Cisco Global Cloud Index: Forecast and Methodology, 2011–2016*, in "Global *Cloud* Index (CGI)", (2012)

[49] *Zettabyte* = 10^{21} *byte* = 1 triliardo di *byte*

[50] Fonte: cisco.com

[51] *CAGR*, in "Wikipedia", (2013), http://en.wikipedia.org/wiki/Compound_annual_growthrate

scita dal 2011 sarà di circa cinque volte e mezzo rispetto ai *workload* in *data center* tradizionali.

Una delle ragioni del successo risiede nella sua architettura che evidenzia i vantaggi della condivisione dei servizi rispetto a prodotti tradizionalmente isolati. È utile allora pensare ad un modello di riferimento di *cloud computing* che ne individui e descriva attori, attività e funzionalità. Una tale rappresentazione è chiamata, appunto, il "modello di riferimento del *cloud*"[52].

L'architettura definisce cinque attori principali: *Cloud Consumer,Cloud Auditor, Cloud Provider, Cloud Carrier, e Cloud Broker*. Una sua definizione, mostrata in figura 10 e curata dal *National Institute of Standards and Technology* (NIST), offre un valido contributo fornendo una chiara comprensione delle tecnologie e dei servizi di *cloud computing.*

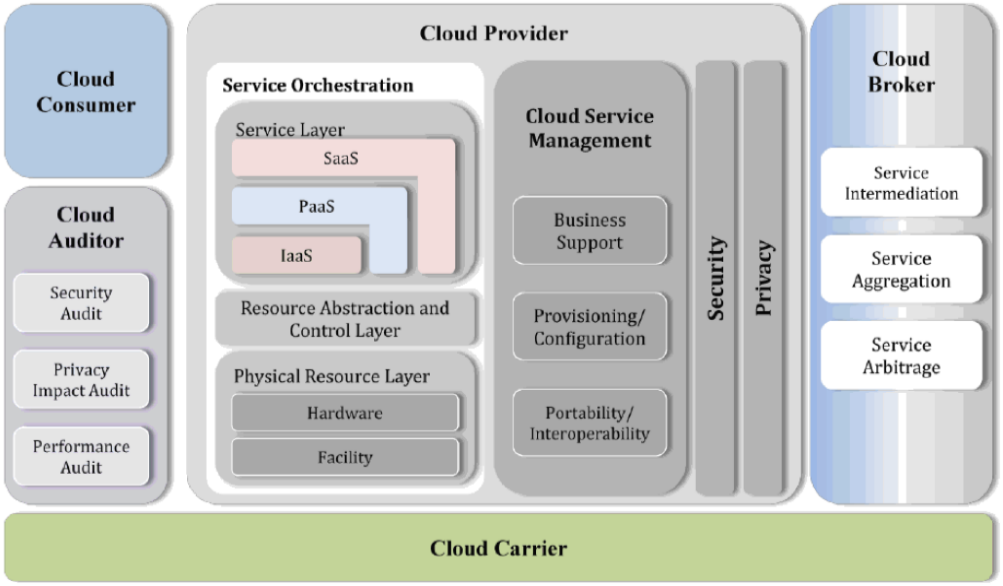

Figura 10: Il modello di riferimento concettuale[53]

Ciascun attore, utente finale o organizzazione, è interessato da processi nel *cloud computing*. La tabella 1 fornisce una breve descrizione dei ruoli.

[52] NIST, *NIST Cloud Computing Reference Architecture*, in Special Publication 500-292 (2011), p. 3

[53] Fonte: nist.gov

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Tabella 1: attori nel *cloud computing*[54]

Tipicamente un *Cloud consumer* interagisce e richiede servizi da un *Cloud Provider*. Quest'ultimo gestisce l'infrastruttura computazionale, fisica e virtualizzata, offrendo modelli di servizio di tipo *Software as a Service* (Saas), *Platform as a Service* (Paas) e *Infrastructure as a Service* (Iaas), con l'ausilio di funzioni interne che sono necessarie per la gestione e il funzionamento (gestione del cliente, report, fatturazione, allocazione automatica delle risorse *cloud* per servizio, possibilità per il *consumer* di spostare i propri dati da e verso molteplici *cloud* provider) il tutto garantendo sicurezza e privacy. Il *consumer* può anche relazionarsi direttamente con un *Cloud Broker* che riformula e commercializza in nuovi servizi quelli di uno o più *provider*. Compito dell'*auditor* è quello di valutare sicurezza, privacy e performance nell'implementazione del servizio *cloud*, interagendo sia lato *consumer*, sia lato *provider*. In tutte le combinazioni interviene il *carrier* a garantire connettività e trasporto dei servizi *cloud* dal *provider* al *consumer*.

Un esempio di servizio *cloud* può essere quello richiesto da un'azienda che si occupa di *e-learning* e che si specializza nello sviluppo di strumenti per la formazione dei propri clienti (piattaforme e applicazioni per corsi online e valutazioni), quali scuole e centri per l'apprendimento.

L'azienda richiede un *Cloud Provider* che possa offrirle risorse computazionali su grandi quantità di dati, capacità per sviluppare le proprie applicazioni e spazio per la memorizzazione dei contenuti, con funzione di indicizzazione e ricerca, oltre alla capacità di bilanciare il carico durante la gestione dei clienti. Un *provider* IaaS e PaaS consentirebbe di ridurre i costi di

[54] Fonte: nist.gov

sviluppo e di mantenimento di una propria infrastruttura fisica, permettendo al consumer di dedicarsi esclusivamente al proprio *core business*, e di contare su una piattaforma scalabile dinamicamente per accomodare i cambiamenti sia d'uso, sia di picco di traffico. Inoltre, i vantaggi della virtualizzazione consentirebbero all'azienda di ridurre i tempi di rilascio di prodotti e servizi *online*, il c.d. *time to market*, rispetto ai tempi necessari usando *hardware* fisico. Google con Picasa offre un sistema *cloud* a misura di singolo utente per l'*editing* e la condivisione di immagini su *cloud* e YouTube per la condivisione di contenuti video. Non si ha necessità di investire in *hardware*/*software* e non vi è dipendenza dalle piattaforme.

1.6 Modelli di servizio: dall'infrastruttura alle applicazioni

Il modello a tre livelli, definito *Service Orchestration* nella figura 10, descrive un'associazione di componenti del sistema con funzioni di coordinamento e gestione delle risorse computazionali dell'infrastruttura *cloud*, unite a tecnologie di virtualizzazione che oramai sono una componente essenziale del *cloud computing* per fornire i *service* al *consumer*[55].

Un'altra sua rappresentazione ad alto livello in termini di *stack*[56] hardware/*software* è quella proposta nella figura 11 dalla *Cloud Security Alliance*. Spostandosi verso l'alto nella pila, ogni modello di servizio (IaaS, PaaS, SaaS) eredita le funzionalità del modello di servizio sottostante.

[55] H. SABOOWALA, M. ABID, S. MODALI, *Design Network and Services for the Cloud*, Ciscopress, 2013, chapter 3

[56] B. KEPES, *UnderstandingThe Cloud Computing Stack SaaS, Paas, IaaS*, (2011), http://broadcast.rackspace.com/hosting_knowledge/whitepapers/Understanding-the-*Cloud-Computing*-Stack.pdf

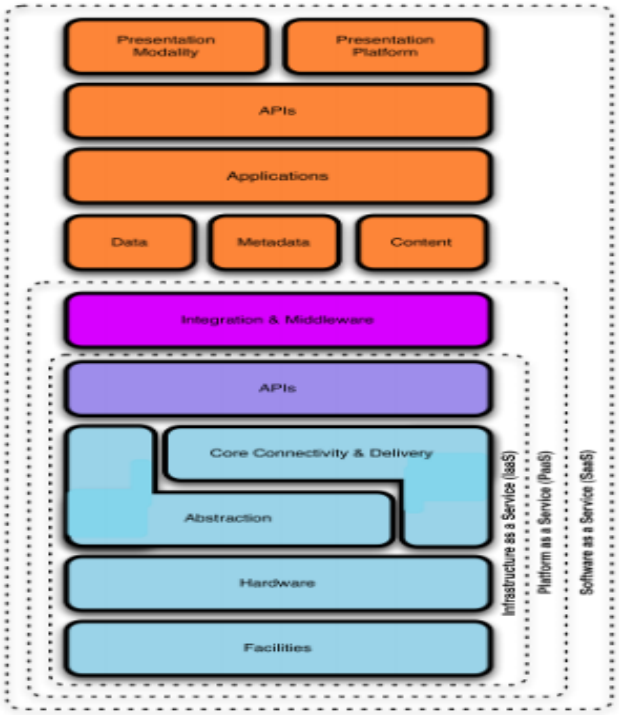

Figura 11: Modello di riferimento[57]

SaaS fornisce servizi agli utenti finali, mentre IaaS e PaaS offrono servizi a ISV[58] e sviluppatori. IaaS ha il minor livello di funzionalità integrate dal provider. In questo modello il *consumer* ha la responsabilità di proteggere i sistemi operativi, le applicazioni e i contenuti perché, al contrario del SaaS, più si scende verso il basso e maggiore diventa la responsabilità per implementarli. Il livello top definisce le interfacce utente e le API[59] tra il consumer e i tre tipi di servizi. Ogni *vendor* ha il suo *set* proprietario di API, molto spesso, non standard. Questo limita l'interoperabilità tra provider e può condurre all'API *lock-in*[60].

Il livello intermedio offre funzioni di *middleware* tramite una *virtual appliance*, ad esempio una applicazione *webserver* eseguita su una macchina virtuale che espone le proprie funzionalità attraverso delle API, oppure un'applicazione *framework* per lo sviluppo.

Il livello inferiore ha capacità di astrarre risorse e di far si che ci sia la connettività fisica e logica a queste risorse. Un *hypervisor* consente ai diver-

[57] Fonte: *Cloud Security Alliance*

[58] ISV = *Independent Software Vendor*

[59] API = *Application Programming Interfaces*, consentono al software di richiedere dati e computazione da uno o più servizi attraverso una interfaccia

[60] *Lock-in* = essere legati e dipendere dalle tecnologie del *vendor*

si sistemi operativi di gestire un proprio spazio di memoria e di I/O per le macchine virtuali e un *set* di API, fornite dal *provider*, ne permette la gestione e l'interazione con l'infrastruttura fisica (CPU, memoria, dispositivi di rete e interfacce, sistemi di *storage*, impianti di riscaldamento/ventilazione, ecc).

Il primo modello di servizio di *cloud computing*, denominato *Infrastructure as a Service* (IaaS), abilita la virtualizzazione dell'*hardware* nel *cloud*, fornendo l'infrastruttura informatica come un servizio. Il *provider* offre la propria infrastruttura fisica (*server*, *storage*, networking, tecniche di bilanciamento del carico, ecc) unita ad una piattaforma di virtualizzazione e connettività. L'utente crea *hardware* analogo, ma privato e virtuale, necessario a ricreare un ambiente virtualizzato su cui "poggiare" le proprie applicazioni e servizi. In sostanza, un fornitore di IaaS crea un servizio di utilità *hardware* tecnologicamente avanzato, che consente di disporre di risorse virtuali su richiesta, queste ultime vengono reindirizzate all'infrastruttura reale del data center, che materialmente esegue le operazioni. Ad esempio un ISV potrebbe usare una soluzione IaaS per accedere ad una rete di *web server* virtuali che le facilitano lo sviluppo e il *testing* delle sue applicazioni, su *hardware* e sistemi eterogenei, che poi distribuirà come infrastruttura. Oppure un fornitore IaaS potrebbe mettere a disposizione un *cluster* computazionale per il calcolo parallelo, spazio di memorizzazione per il *backup*, soluzioni di *disaster recovery* o *data center* privati virtuali. In questo caso giocano un ruolo fondamentale i servizi di rete virtualizzati, necessari nella rete per supportare il *cloud computing*, quali bilanciamento del carico, *firewalling*, IDS/IPS[61] e VPN[62].

L'utente paga per la capacità del sistema realmente consumata e mantiene la gestione della propria infrastruttura virtuale tramite un'interfaccia *Web Service* che gli consente il controllo delle risorse computazionali e la possibilità di ridurre i tempi per il *deploy* di nuove funzionalità, delegando al provider operazioni di *hosting* e di gestione dell'infrastruttura fisica. Un *Web Service* è un sistema *software* progettato per supportare l'interazione "macchina-a-macchina" che avviene in una rete. Può esserci sia un utente che fa richiesta di un servizio da un *Web Service*, sia un W*eb Service* che richiede

[61] IDS = *Intrusion DetectionSystem*. IPS = *Intrusion Prevention System*

[62] VPN = *Virtual Private Network*

un servizio da un altro *Web Service*[63]. I *Web Service* utilizzano, per comunicare, messaggi SOAP (un protocollo di messaggistica basato su XML), trasmessi attraverso il protocollo HTTP[64]. Tra i tanti esempi si possono annoverare gli *Amazon Web Services* (AWS), tra i più popolari IaaS del momento, che, grazie alla virtualizzazione *hardware*, rendono possibile la creazione di *server* virtuali privati, su sistemi operativi Windows Server e Linux, che possono essere eseguiti ovunque Amazon EC2)[65], oppure un sistema di *storage* di tipo "gestito" per l'archiviazione di dati o *backup* disco (Amazon S3)[66].

Il *Platform as a Service* (PaaS) è un modello di servizio di *cloud computing* dove il *cloud consumer* è prevalentemente interessato a sviluppare ed eseguire applicazioni *software*. Per questo richiede al *provider* una piattaforma operativa che includa il *middleware*, con un ambiente di *runtime* su cui avviare le applicazioni o un *database* e strumenti di sviluppo, senza preoccuparsi del costo e della complessità di gestione della piattaforma. Il modello PaaS consente di gestire l'intero ciclo di vita del *software*, dalla costruzione al *delivering*, permettendo al cliente di concentrarsi sullo sviluppo *"web based"* e il *deploy* sulla sottostante architettura *hardware*/*software*, gestita ora dal *provider* (*network*, *server*, sistemi operativi o *storage*), utilizzando le API implementate e configurate da remoto. Molto spesso la soluzione PaaS è parte integrante di un modello IaaS, in questo caso il *provider* offre al cliente la possibilità di accesso diretto a *server* virtuali utilizzabili per sviluppo e test, così da avere il governo dell'implementazione delle risorse virtuali su IaaS.

Alcuni esempi di PaaS includono: *Google App Engine* che rappresenta un sistema per la distribuzione di *web application* su infrastruttura Google; *Force.com* che consente di sviluppare in Apex (una variante Java), utilizzando una sintassi XML per la creazione di interfacce utente in HTML, Ajax e Flex; *Microsoft Azure* che permette agli sviluppatori di avere una piatta-

---

[63] W3C, *Web Services Architecture*, in W3C Working Group Note 11 February 2004, http://www.w3.org/TR/ws-arch/

[64] P. JITHIN, S. K. V. JAYAKUMAR, *Performance comparison of web service in IaaS cloud and standard deployment model*, in International Journal of *Computer* Trends and Technology (IJCTT), 2013, vol. 4(6), pp. 1589-1593

[65] *EC2*, in *Amazon Elastic Computer Cloud* (Amazon EC2), http://aws.amazon.com/ec2/

[66] *S3*, in *Amazon Simple Storage Service* (Amazon S3), http://aws.amazon.com/s3/

forma che usi il *framework* .NET, che supporti SQL *Server* e che sia programmabile all'interno di Visual Studio.

L'ultimo livello di servizio di *cloud computing*, probabilmente il più conosciuto, è il *Software as a Service* (SaaS). Il suo focus è la distribuzione di *software*, con le applicazioni che sono ospitate dal *cloud provider* e rese disponibili al *consumer* tramite una rete tipicamente Internet, fruibili il più delle volte con un *web browser on demand*. Il cliente è trasparente rispetto alla sottostante piattaforma ospite e all'infrastruttura fisica e virtuale del *cloud*, ha solamente il controllo sull'applicazione che gli viene distribuita e su alcune configurazioni dell'ambiente di *hosting* che la ospita.

Il modello SaaS consente di ottenere gli stessi benefici funzionali del *software* tradizionale eseguito localmente nei *server* interni, ma senza i problemi legati al possesso dell'*hardware*, all'installazione e gestione delle licenze, al supporto per gli aggiornamenti e alle *patch*. Un altro vantaggio è quello di offrire un accesso al servizio, per i dipendenti di un'organizzazione, che sia globale. Per tutti loro il *software* avrà la stessa versione, lo stesso grado di protezione e il formato dei dati sarà per tutti compatibile, il tutto con una riduzione dei costi, dei rischi che ora sono affidati al *provider* e del tempo di implementazione dell'applicazione e del *roll out* dei cambiamenti.

Molte tipologie di *software* si prestano al modello SaaS quali: CRM[67] per vendite, *marketing* e servizi al cliente, video conferenza, *email*, strumenti di *web collaboration* ecc. Le applicazioni SaaS sono progettate per l'uso concorrente di una singola istanza (*multi-tenancy*) in contrapposizione alle soluzioni dei provider ASP, che, per certi versi, avevano diverse analogie con le attuali SaaS, però si presentavano come operatori dedicati ad un particolare cliente. Molte soluzioni SaaS offrono delle API per consentire un certo grado di personalizzazione. Un esempio di SaaS è la *suite Google Apps* con servizi di *word processing*, *calendar* ed *email*.

[67] CRM = *Customer Relationship Management*

1.7 Modelli di implementazione e tipologie di *cloud*

Il *cloud computing* propone diversi modelli per la sua implementazione, ovvero particolari metodi per fornire un servizio, e sulla base di questo se ne definiscono i confini.

I modelli più comunemente utilizzati sono i seguenti: *Public Cloud*, *Private Cloud*, *Hhybrid Cloud*, *Community Cloud*[68]. Il *Public Cloud* si riferisce a servizi IT erogati da un *provider* a diversi soggetti esterni, il *Private Cloud* opera in esclusiva solamente per un'unica organizzazione, il modello ibrido combina tra loro aspetti di due o più tipologie di *cloud*, mentre il *Community Cloud* propone un'infrastruttura condivisa tra diverse organizzazioni a supporto della loro stessa comunità. Da precisare che questi quattro modelli non sono legati alla locazione fisica dell'infrastruttura o dell'applicazione, uno stesso *data center* potrebbe implementare *cloud* di diverso tipo. In effetti un modello di servizio descritto in precedenza, quale il SaaS, può essere offerto agli utenti in una o più classi di implementazione, per esempio *public* o *private*.

In particolare, i *public cloud* (o *cloud* pubblici) sono gestiti da un *provider* che mette a disposizione dei vari *consumer*, detti anche *tenant* i suoi servizi, fornendo un accesso Internet ad un *pool* di risorse dedicate (*single-tenant*) o condivise (*multi-tenant*). L'infrastruttura tecnologica del *data center* è generalmente di proprietà e sotto il controllo del fornitore di servizi *cloud*. Si tratta di una piattaforma elaborativa flessibile e altamente scalabile, con accesso ad alta banda alle risorse delle macchine virtuali necessarie al cliente e caratterizzata dal pagamento delle ore effettivamente utilizzate. Dal

[68] S. CARLIN, K. CURRAN, *Cloud Computing Security*, International Journal of Ambient *Computing* and Intelligence, 3(1), 2011, pp. 15-16. Le principali tipologie di *cloud computing* sono state successivamente descritte anche nell'allegato al parere n. 5/2012 "*ex* Art. 29 per la protezione dei dati dell'Unione Europea". Anche l'Autorità Garante per la protezione dei dati personali ha descritto le principali tipologie di *cloud computing* in due distinti documenti: "*Il Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*", pubblicato (in data 16 novembre 2011 e consultabile all'indirizzo web http://garanteprivacy.it/web/guest/home /docweb/-/docweb-display/docweb/1819933) e il successivo "*Cloud Computing: proteggere i dati per non cadere dalle nuvole*" (pubblicato in data 24 maggio 2012 e consultabile all'indirizzo web http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1894503). Sui documenti sopraccitati si tornerà nella parte terza e quinta del presente lavoro.

punto di vista di un'organizzazione risulta conveniente in quanto non si devono affrontare i costi di investimento dell'infrastruttura IT e dello staff altamente specializzato.

Il *private cloud* rappresenta, invece, l'infrastruttura di *cloud* privata utilizzata per l'uso esclusivo di un'organizzazione. Quest'ultima ne gestisce l'operatività all'interno dei confini della propria *enterprise* oppure può delegarla ad un *provider*. In quest'ultimo caso parte delle potenzialità della struttura virtuale del *cloud* pubblico sarà messa a disposizione del cliente in forma esclusiva (tipicamente attraverso uno spazio di indirizzamento privato e un *firewall* e una VLAN privata oppure fisicamente separando le zone)[69], un esempio potrebbe essere un *cloud* privato virtuale, termine che descrive un concetto simile a quello di rete privata virtuale (VPN), ma applicato al *cloud computing*.

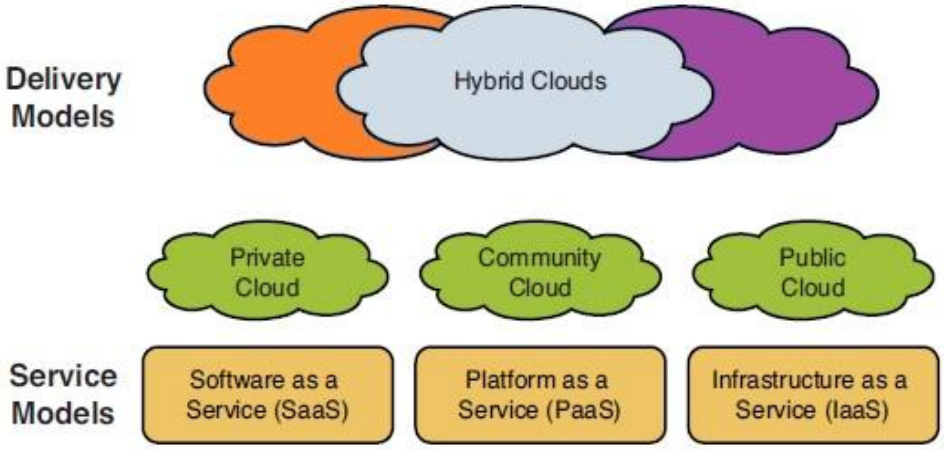

Figura 12: Modello di implementazione[70]

Si presume, inoltre, che un *cloud* privato, interno al reparto IT, non utilizzi lo stesso livello di virtualizzazione o evoluzione tecnologica che un provider di *cloud computing* può raggiungere, anche se in alcuni casi si richiede che i dati siano sotto il controllo di un unico soggetto, preferendo quindi non esternalizzare. In entrambi i casi l'implementazione privata consente al *consumer* un maggiore controllo sulla qualità del servizio offerto, non dovendolo condividere come avviene per il pubblico, potendo contare

[69] Cisco Systems, *Securing Networks with Private VLANs and VLAN Access Control Lists*, in "Cisco Catalyst 6000 Series Switches", (2008), http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/10601-90.html

[70] Fonte: nist.gov

su più alti livelli di supporto da parte del *provider* e, magari, non accedendovi da un rete *"best effort"* quale è Internet, ma tramite una rete WAN, anch'essa privata. Certamente, come detto, una soluzione privata appare in linea con le necessità di una grande organizzazione o agenzia governativa di non esternalizzare le attività critiche, piuttosto che di una piccola realtà, a causa degli alti costi iniziali di *startup* e di operatività a regime.

Quando un'organizzazione di livello *enterprise* si affida al *hybrid cloud*, allora combina i servizi di due o più tra *cloud* pubblico, privato e di comunità. I tre modelli restano separati, sia dal punto di vista della posizione, perché possono coesistere nello stesso *data center* o geograficamente separati, sia dal punto di vista delle loro peculiarità di *performance*, affidabilità e sicurezza, ma legati dal punto di vista tecnologico in modo da consentire la portabilità dei dati tra loro, ossia la possibilità di "muovere" applicazioni e dati attraverso sistemi di *cloud computing* tra diversi *provider*. Si può beneficiare così della scalabilità tipica del pubblico e dell'alto grado di controllo offerta dal privato. Per esempio potrebbe demandare in *outsourcing* i servizi di archiviazione e *backup* all'esterno, presso un *provider* di *cloud* pubblico oppure utilizzarlo in *realtime* in caso di picchi di domanda, mantenendo i normali *workload* nel privato (*cloud bursting*)[71].

Infine, l'implementazione *community cloud* prevede la partecipazione di membri appartenenti a una o più organizzazioni che collaborano alla stessa *mission.* Può essere gestito dalla stessa comunità oppure da una parte terza, fuori sede. Ogni partecipante definisce un nodo anche geografico del *cloud* e il fatto di non dipendere da una sola organizzazione facilità un minore *down time* in caso di *failure*, gli altri nodi possono momentaneamente compensare il disservizio.

Un esempio di questo modello lo fornisce il portale Info.apps.gov[72], a cura dell'agenzia indipendente *General Services Administration* (GSA), che fornisce servizi all'amministrazione degli Stati Uniti. In questo caso la *community* è formata dall'insieme delle agenzie federali governative che vi partecipano, usufruendo dei servizi di *cloud computing* per il governo federale.

[71] *Cloud bursting*, in "Wikipedia", (2013), http://en.wikipedia.org/wiki/*Cloud_computing*

[72] *info.apps.gov*, in http://cloud.cio.gov

1.8 I vantaggi

Alcuni dei vantaggi derivanti dall'utilizzare una soluzione *cloud computing* sono riassunti di seguito[73].

- Riduzione dei costi. Grazie alla virtualizzazione, al consolidamento delle risorse fisiche e considerato che tutta l'elaborazione avviene sui *server* del *cloud*, non c'è alcuna necessità, per l'utente, di investire in *computer* tradizionali. Basteranno dispositivi *client* dal costo limitato per collegarsi.

- Migliori prestazioni. Con l'elaborazione che viene eseguita sui *cluster* di *server*, gli utenti potranno avere prestazioni migliori rispetto ai *computer* tradizionali.

- Facilità di utilizzo. A seconda del tipo di servizio offerto potrebbero non essere richieste licenze *hardware* o *software* per implementarlo.

- Compatibilità dei formati. Considerato che le applicazioni sono ospitate presso il *provider*, l'utente non dovrà preoccuparsi della compatibilità dei suoi documenti con l'applicazione di un altro utente del *cloud* o sistema operativo. Questo facilita anche la *collaboration*, dal momento che i *file* sono nel *cloud*, allora tutti gli utenti autorizzati hanno accesso agli stessi *file*.

- Spazio di archiviazione virtualmente infinito. Il grande beneficio nel *cloud* è l'enorme spazio a disposizione per l'uso.

- Indipendenza dal dispositivo. L'accesso al *cloud computing* è indipendente dal dispositivo. Non è necessario utilizzare un *computer* o un dispositivo specifico per accedere ai dati. Fino a quando vi sarà la connettività Internet sarà possibile raggiungere dati e applicazioni.

- Affidabilità. La caratteristica di avere un'architettura scalabile, la capacità di fornire il bilanciamento del carico sia all'interno del *data center* che tra *data center* del *cloud* e il rapido ripristino in caso di *failure*, lo rende estremamente affidabile.

- Gestione IT in *outsourcing*. A seconda del modello di distribuzione del *cloud computing*, questo consente a qualcun altro di gestire l'infrastruttura informatica, ottenendo una notevole riduzione dei costi del personale tecnico.

---

[73] M. CARROL, P. KOTZE', A. van der MERWE, *Securing Virtual and Cloud Environments*, in *Cloud Computing and Services Science*, Springer, 2012, p. 78-79

-Manutenzione e aggiornamento semplificati. Poiché il sistema è centralizzato, si possono facilmente applicare patch e aggiornamenti. Tutti gli utenti avranno sempre accesso alle ultime versioni del *software* e non dovranno preoccuparsi di farlo personalmente.

1.9 Criticità

Generalmente possiamo pensare che i vantaggi del *cloud computing* siano più apprezzati dalle piccole organizzazioni piuttosto che dalle grandi. Le organizzazioni più grandi sono, infatti, in grado di supportare i costi del personale e dello sviluppo IT, necessari per le proprie soluzioni ad hoc. Di seguito alcuni fattori che possono esser considerati dei freni al suo sviluppo[74].

- Livello di personalizzazione. Quando si utilizza un'applicazione o un servizio del *cloud*, normalmente non è così personalizzabile come si vorrebbe. Inoltre, molto spesso le applicazioni distribuite in locale hanno ancora molte più funzioni rispetto alle analoghe nel *cloud* (ad esempio con Microsoft Word sul proprio PC si possono avere molte più funzioni rispetto a quelle fornite da Google Docs), questo anche per compensare eventuali limitazioni nella banda.

- Connessione a Internet costante. In mancanza di connettività non si accede ai servizi *cloud* e le applicazioni non saranno disponibili, a meno di avere un backup dei dati sui propri sistemi locali o un collegamento alternativo con un secondo fornitore d'accesso. Tuttavia con l'avvento di tecnologie wireless come Wi-Fi, WiMAX e nella telefonia mobile 3G e 4G, l'accesso a Internet sta diventando un problema minore.

- Banda limitata. Il *cloud computing* richiede connessioni a banda larga, la ridotta larghezza di banda in località poco servite, le distanze WAN da percorrere (latenza) o la congestione della rete, compromettono le prestazioni.

-Sicurezza. Fattori di notevole interesse nel *cloud computing* sono indubbiamente la privacy e la sicurezza. Quando i dati fluiscono nel *cloud* e

[74] M. MILLER, *Cloud Computing*: Web-based applications that change the way you work and collaborate online, Que publishing, 2008

risiedono su sistemi che non sono più sotto il controllo diretto dell'utente, aumenta il rischio per la loro integrità.

PARTE SECONDA - SICUREZZA E CONTROLLO DEI SERVIZI IN *CLOUD*

1. Aspetti di sicurezza nel *Cloud computing*

1.1 Problematiche generali

Attualmente si sta vivendo una fase storica di rapida espansione nel desiderio di connettività da qualsiasi dispositivo verso molti *cloud* e questo sta avendo un impatto significativo nel panorama delle minacce alla sicurezza, seguito da problematiche riguardanti la conformità, la privacy e le questioni legali. Sono in continuo aumento gli utenti che, da qualsiasi luogo, utilizzano diversi dispositivi con accesso a Internet per collegarsi a varie reti e servizi in esecuzione ovunque, in un *cloud* SaaS pubblico, in un *cloud* privato o in uno ibrido, attraverso una vasta gamma di applicazioni, mentre *software* e dati sono memorizzati sui *server*, esponendoli però alle vulnerabilità. Anche se ci sono molti vantaggi nell'adottare i servizi *cloud*, ci sono anche alcune significative barriere d'ingresso. Questo perché ancora il *cloud computing* rappresenta un paradigma relativamente nuovo. Vi è ancora una certa incertezza su come la sicurezza a tutti i livelli (ad esempio rete, *host*, applicazioni e dati) possa essere raggiunta e in che modo la sicurezza delle applicazioni debba ora essere spostata verso il *cloud computing*.

Le maggiori preoccupazioni degli utenti riguardano la perdita di dati e i rischi per la privacy, seguite dai rischi di sicurezza in generale, e la rivendicazione dei diritti di proprietà intellettuale. Altre sfide chiave per la sicurezza, anche se meno sentite, sono la conformità dal punto di vista legale e normativo, la disponibilità del sistema e la *business continuity*[1]

Cinque punti centrali, che verranno continuamente analizzati e riproposti da qua in avanti, in generale rappresentano delle vere e proprie sfide che gli

[1] KPMG, *The cloud takes shape. Global cloud survey: the implementation challenge*, (2013), p.15

operatori del settore stanno cercando di affrontare per rassicurare i propri clienti:

- Sicurezza. Assicurarsi che ci siano sufficienti misure minime di sicurezza nei livelli di protezione che il *provider* fornirà e gestirà, tali dagiustificare la riservatezza, l'integrità e la disponibilità di tutte le informazioni che dovrà tenere memorizzate o trasmettere.

- Controllo. Nel *cloud* le possibilità di controllo sono meno definite. Gli utenti sono sempre più interessati nel sapere se manterranno il controllo su come e dove muovere i propri dati, oltre ad avere certezza della loro eliminazione definitiva una volta concluso il servizio. Non possedendo e gestendo il *data center* di proprietà e non potendolo localizzare geograficamente, risulta loro difficile pensare di implementare delle reti di sicurezza attorno ai propri dati, così come applicare strumenti quali *firewall* e *software antivirus*, dato che non possono definire facilmente il perimetro della rete, causa infrastruttura distribuita, *multi-tenancy* e virtuale. Per farlo devono affidarsi al *provider*.

- Gestione del livello di servizio. Occorre garantire, con un opportuno monitoraggio delle misurazioni effettuate sui singoli parametri di qualità, che ciascuna applicazione o servizio possa ottenere le risorse e le priorità necessarie ad essere eseguita nel *cloud*, secondo le promesse contrattualizzate (si veda la trattazione su SLA nella parte quinta), al fine di pianificare capacità e *business continuity*, in evenienza di criticità quali caduta di prestazioni, guasti o attacchi.

- Conformità. Verificare che il *cloud* sia conforme alla normativa nazionale e internazionale e che questa assicuri un elevato livello di tutela nel trattamento dei dati, sia essi memorizzati o trasferiti all'estero.

- Interoperabilità e portabilità. L'implementazione di un sistema di *cloud computing*, nella sua evoluzione, dovrebbe puntare a non diventare un sistema chiuso, ovvero dovrebbe fornire la possibilità ai propri servizi di interagire con quelli di altri sistemi *cloud* e consentire ai dati e alle applicazioni di essere trasferiti da un sistema ad un altro secondo standard comuni, evitando che gli utenti rimangano vincolati ad un solo *provider* e quindi prevenendo il *vendor lock-in*. L'incompatibilità tra sistemi proprietari, con differenze tec-

nologiche negli *hypervisor* e nelle API, contribuisce al venir meno di questi requisiti[2].

L'avvento quindi del *cloud computing* impegna tutti gli operatori ad ogni livello, il tutto è accelerato dal processo in atto di fornire accesso Internet a persone, processi, dati e oggetti di ogni tipo, così come indicato da Cisco nella definizione di *Internet of Everything* (IoE)[3].

1.2 La sicurezza nei tre modelli di servizio

Il modello *cloud* offre tre modelli di servizio, che, come visto nel primo capitolo, sono[4]:

-*Infrastructure as a Service* (IaaS). Il servizio offerto al *consumer* è quello di poter gestire personalmente risorse di: elaborazione, memorizzazione dei dati, *networking*, e altre in cui poter poi distribuire ed eseguire *software*, inclusi sistemi operativi e applicazioni.

-*Platform as a Service* (PaaS). Il servizio offerto al *consumer* è quello di poter sviluppare e distribuire, sull'infrastruttura *cloud*, le proprie applicazioni senza dover installare alcuna piattaforma o *tool* di sviluppo sulle proprie macchine locali. PaaS fornisce il supporto del sistema operativo e del *framework* di sviluppo *software*.

-*Software as a Service* (SaaS). Il servizio offerto al *consumer* è quello di utilizzare le applicazioni del *provider* in esecuzione su un'infrastruttura *cloud* di proprietà di quest'ultimo. Le applicazioni sono accessibili da vari dispositivi *client* attraverso un'interfaccia *thin client*[5], come un *browser web*, per esempio la posta elettronica *"web-based"* di Google[6].

---

[2] C.PAHL, LI ZHANG, F.FOWLEY, *A Look at Cloud Architecture Interoperability through Standards*, in CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013, pp. 7-12

[3] Cisco Systems, *Internet of Everything*, in http://www.cisco.com

[4] A. MALIK, M. M. NAZIR, *Security Framework for Cloud Computing Environment: A Review*, in Journal of Emerging Trends in *Computing* and Information Sciences, vol.3, n. 3, (2012), pp. 390-391

[5] *Thin client*, in "Wikipedia", (2013), http://it.wikipedia.org/wiki/Thin_client

[6] *Google Gmail*, https://mail.google.com/mail/help/intl/it/about.html

Ciascun modello presenta le sue criticità. PaaS così come SaaS sono servizi che poggiano su IaaS, quindi ogni violazione a livello IaaS avrà un impatto sulla sicurezza degli altri servizi. In questa sezione ci limitiamo a presentare le macro categorie di interesse in termini di sicurezza, presenti in ciascuno dei tre modelli di servizio. Successivamente verranno segnalate le criticità con una panoramica su vulnerabilità, minacce e rischio a seguito di attacco.

Con il modello SaaS si ha il maggior grado di astrazione rispetto all'infrastruttura sottostante, in genere un'offerta SaaS presenta un elevato grado di funzionalità integrate direttamente nella soluzione *cloud*, compresa la sicurezza, quindi con il minor livello di estensibilità per il cliente. Questo comporta che la gestione del rischio è curata principalmente dal *provider*. Sarà suo compito, in un sistema *multi-tenancy*, tenere isolate le istanze di più utenti e fare in modo che ciascuno veda e acceda solamente alle risorse delle proprie *virtual machine*. Dovrà garantire la sicurezza delle *web application* offerte ai propri clienti, eliminando eventuali vulnerabilità sia a livello *software* che di rete, per evitare che possano essere lanciati degli attacchi *web* dall'esterno. Proteggerà l'integrità dei dati con efficaci misure di autenticazione, autorizzazione e con robusti algoritmi di cifratura, oltre che con un'adeguata pianificazione di *backup* e ridondanza dei dati, al fine di garantirne la disponibilità. In tutto questo il *tenant* non percepisce quali siano le misure di sicurezza globale applicate dal *provider* all'intera piattaforma. Per di più, il *software* SaaS del *provider* potrebbe essere ospitato presso la sua stessa infrastruttura fisica oppure in un IaaS di terzi. Quindi il cliente soffre la perdita di controllo e di conoscenza su dove effettivamente risiedano i suoi dati.

Per contro, il modello PaaS offre all'utente una maggiore estensibilità e un maggiore controllo sulla piattaforma. La messa in sicurezza del livello PaaS comporta sia la sicurezza della piattaforma stessa e quindi dei *runtime engine* sui quali vengono eseguite le applicazioni sviluppate, sia la sicurezza delle applicazioni create e il loro *deployment* nella piattaforma. L'utente PaaS è uno sviluppatore che cura l'intero ciclo di vita delle proprie applicazioni, inclusa la sicurezza.

IaaS, per il livello relativamente basso di astrazione, consente il massimo grado di gestione e personalizzazione dei servizi e della sicurezza, più di quanto non facciano PaaS o SaaS[7].

Sappiamo che IaaS mette a disposizione un *pool* di risorse quali *server*, *storage*, servizi di rete in forma virtualizzata, quindi bisogna prestare attenzione alle eventuali vulnerabilità delle *virtual machine* edell'*hypervisor*, che in un contesto di condivisione delle risorse quale è quello offerto dal *multi-tenancy*, risultano critiche.

Si evidenzia, quindi, che in uno scenario in cui intervengono soggetti diversi, ogni *provider* sarà responsabile nel garantire i propri servizi, tramite strumenti di protezione che sono tipici del contesto a cui vengono applicati. Questo può causare una combinazione incoerente di modelli di sicurezza e può rendere opaco quale provider ne sia responsabile a seguito di attacco[8].

Per queste ragioni, alcune organizzazioni internazionali, spesso non-profit, tra cui *Cloud Security Alliance* (CSA) e governative quali il *National Institute of Standard and Technology* (NIST) e *l'European Network and Information Security Agency* (ENISA), forniscono informazioni e promuovono l'uso di *best practice* in ambito sicurezza, privacy e normativa del *cloud computing*[9], che saranno descritti dettagliatamente nelle prossime sezioni.

1.3 Domini di sicurezza identificati da CSA

Cloud Security Alliance[10] è una organizzazione non profit formalmente creata nel Dicembre 2008, a seguito di una serie di incontri organizzativi con i leader del settore e ora sostenuta da un gran numero di associazioni e aziende IT. La sua *mission* è quella di fornire competenze per affrontare tutti gli aspetti della sicurezza *cloud*, tra cui la conformità agli standard, la legislazione e regolamentazione in materia di sicurezza e la formazione. Negli

[7] B. KANDUKURI, R. PATURI, A. RAKSHIT, *Cloud Security Issues*, in IEEE International Conference on Services *Computing*, (2009)

[8] K. CURRAN, S. CARLIN, M. ADAMS, *Security issues in cloud computing*, in Elixir Network Engg 38, (2011)

[9] S. SEONGHAN, K. KAZUKUNI, *Towards Secure Cloud Storage*, in Demo for CloudCom2010, (2010), p. 1

[10] *Cloud Security Alliance*, https://cloudsecurityalliance.org/

ultimi tre anni è diventata il punto di riferimento per gli standard di sicurezza a livello globale, ratificati poi dagli organismi internazionali preposti.

CSA ha pubblicato la prima bozza della "*Security Guidance for Critical Areas of Focus in Cloud computing*" nell'aprile 2009. Questa guida fornisce informazioni su come approcciare al paradigma del *cloud* e sugli aspetti di sicurezza nelle piattaforme di *cloud computing*. Nel 2011 è stata rilasciata l'attuale ultima terza versione[11].

La guida è divisa in quattordici domini allineati secondo gli standard industriali e le *best practice* in materia di *cloud*, il primo dominio denominato *Architectural Framework* fornisce alcune informazioni sulla piattaforma di *cloud computing* e un modello di riferimento dal punto di vista della sicurezza. Il resto dei tredici domini è suddiviso in due principali categorie denominate G*overnance* e *Operation*. La categoria *Governance* affronta questioni strategiche quali interoperabilità e portabilità e di *policy* sulle piattaforme di *cloud computing*, mentre la categoria *Operation* si concentra più tecnicamente sui rischi per la sicurezza e l'applicazione dei concetti all'interno dell'architettura. Le 13 aree critiche sono elencate nella tabella 2:

Domini della categoria *Governance*	**Domini della categoria *Operation***
1. Governance and Enterprise Risk Management	6. Traditional Security, Business Continuity and Disaster Recovery
2. Legal Issues: Contracts and Electronic Discovery	7. Data Center Operations
3. Compliance and Audit	8. Incident Response, Notification and Remediation
4. Information Management and Data Security	9. Application Security
5. Portability and Interoperability	10. Encryption and Key Management
	11. Identity and Access Management
	12. Virtualization
	13. Security as a Service

Tabella 1: Aree critiche individuate da CSA[12]

[11] CSA, *Security guidance for critical areas of focus in cloud computing*, 2011 3°, (2009)

[12] Fonte: *Security Guidance for Critical Areas of Focus in Cloud computing* V3.0

-*Governance and Enterprise Risk Management.* Si concentra sull'abilità di un'organizzazione nel gestire e misurare i rischi associati al *cloud computing*.

- *Legal Issues.* Si occupa di questioni giuridiche connesse alla protezione delle informazioni e dei sistemi informatici, ai requisiti di privacy e alle leggi internazionali.

-*Compliance and Audit.* Riunisce i requisiti di conformità e come questi impattano sulle *policy* di sicurezza interna.

-*Information Management and Data Security*. Tratta la gestione dei dati, come ad esempio la creazione, l'utilizzo, la condivisione, la conservazione, la cancellazione e identifica chi è responsabile della riservatezza, integrità e disponibilità dei dati.

-*Portability and Interoperability.* Descrive gli standard per l'interoperabilità tra i diversi *provider* di *cloud* e la caratteristica dei componenti di un'applicazione nell'essere spostati e riusati altrove, indipendentemente dal nuovo contesto di arrivo.

-*Traditional Security, Business Continuity and Disaster Recovery.*Documenta le procedure di sicurezza tradizionali, i processi di *business continuity* ovvero la continuità operativa dei componenti di una piattaforma *cloud* e di *disaster recovery* per il processo di ripristino da una condizione di emergenza e dove il *cloud computing* possa aiutare a diminuire certi rischi sulla sicurezza.

- *Data Center Operations.* Fornisce informazioni su come si possa valutare il funzionamento di un data center per architettura e operatività, al fine di selezionare il migliore.

-*Incident Response, Notification and Remediation.*Ci aiuta a capire le complessità del *cloud computing* per una corretta gestione degli incidenti e della legislazione tra utente e *provider*.

-*Application Security.* Chiarisce il ciclo di sviluppo del *software* nel *cloud computing*, quali accorgimenti adottare per la messa in sicurezza delle applicazioni e su quale modello di servizio erogarle (IaaS, PaaS e SaaS).

-*Encryption and Key Management.* Indica come proteggere l'accesso ai dati e alle risorse del *cloud*, utilizzando la crittografia e una corretta gestione delle chiavi crittografiche.

-*Identity and Access Management.* Dichiara l'importanza della gestione delle identità e degli accessi al *cloud*. Inoltre, si concentra sulle identità federate, così che ogni utente possa avere una sola identità digitale e con questa accedere a diversi servizi *cloud*.

-*Virtualization.* Esamina le questioni di sicurezza relative alla tecnologia di virtualizzazione, come le vulnerabilità dell'*hypervisor*, i rischi associati al *multi-tenancy* e l'isolamento delle macchine virtuali.

-*Security as a Service*. Indaga il ruolo di fiducia assegnato a terze parti, a cui affidarsi per la garanzia della sicurezza, la gestione degli incidenti, le verifiche di conformità e la gestione dell'identità e accesso.

1.4 Domini di sicurezza identificati dal NIST

Il *National Institute of Standards and Technology*[13] è una agenzia governativa americana che si occupa di promuovere l'innovazione e la competitività degli Stati Uniti. In questo contesto fornisce indicazioni agli utenti sul *cloud computing*, identificando le vulnerabilità relative alla sicurezza. Le questioni di sicurezza e privacy discusse dal NIST sono specificamente riferite ai provider di *cloud* pubblico e sottolineano quali valutazioni dovrebbero fare gli utenti quando affidano in *outsourcing* dati, applicazioni e infrastruttura.

Le sezioni in tabella 3 evidenziano esempi di problematiche generali su privacy e sicurezza che si ritiene abbiano un peso a lungo termine per il *cloud* pubblico[14].

1. Governance
2. Compliance
3. Trust
4. Architecture
5. Identity and Access Management
6. *Software* Isolation

[13] NIST, in "Wikipedia", (2013), http://it.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

[14] NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, in Special Publication 800-144, (2011), p. 14

7. Data Protection
8. Availability
9. Incident Response

Tabella 2: Aree critiche individuate dal NIST[15]

-*Governance.* Definisce linee guida su *policy*, procedure e standard necessarie per l'implementazione e la gestione di servizi *cloud* da parte delle organizzazioni cliente. Nell'affidare questi servizi è richiesta attenzione su ruoli e responsabilità tra cliente e *provider* e raccomandato l'uso di strumenti di *auditing* e gestione del rischio.

-*Compliance.* Si riferisce alla responsabilità di un'organizzazione di operare in accordo con la legislazione attuale, i regolamenti, gli standard e le specifiche, per quanto riguarda la posizione dei dati e la loro gestione, la privacy e i controlli di sicurezza.

-*Trust.* Descrive come una organizzazione, cedendo il controllo diretto su molti aspetti di sicurezza e privacy, conferisce un alto livello di fiducia al *provider*. Per questo motivo il fornitore deve offrire garanzie sulle possibili minacce interne causate dalla condivisione delle risorse tra più utenti e deve operare la gestione del rischio. Il contratto con il cliente deve dichiarare la proprietà dei dati e dei diritti da parte di quest'ultimo.

-*Architecture.* Discute le questioni relative ai sistemi *hardware* e *software* utilizzati dal *cloud computing* e la loro messa in sicurezza, come protezione *dell'hypervisor*, la protezione della rete virtuale con *virtual switch* (vSwitch), la protezione delle macchine virtuali con immagini sempre aggiornate e la protezione lato *client* che il *provider* deve richiedere all'utente.

-*Identity and Access Management.* Segnala l'importanza sulla verifica di identità, autenticazione e controllo di accesso e consiglia di utilizzare *Security Assertion Markup Language* (SAML)[16] per l'autenticazione e *eXtensible Access Control Markup Language* (XACML)[17] per il controllo d'accesso alle risorse.

---

[15] Fonte: nist.gov

[16] OASIS, *Security Assertion Markup Language*, in "*OASIS Security Services*", https://www.oasis-open.org/committees/security

[17] OASIS, *eXtensible Access Control Markup Language*, in "*OASIS Security Services*" https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

-*Software Isolation.* Mette in guardia sui rischi associati al *multi-tenancy*, indipendentemente dal modello di servizio (IaaS, PaaS e SaaS) utilizzato e dell'architettura *software*. Le computazioni di *tenant* diversi devono poter essere svolte in isolamento tra loro, principalmente attraverso l'uso di meccanismi di separazione logici.

-*Data Protection.* Si concentra sulla necessità della riservatezza dei dati e del loro isolamento, dal momento che i dati provenienti da diversi clienti risiedono presso un *data center* comune. I dati devono essere protetti durante la loro archiviazione, in transito e in uso e l'accesso ai dati deve essere controllato.

- *Availability.* Avverte sulle minacce che hanno un impatto negativo sull'accessibilità e uso delle risorse. Interruzioni temporanee o prolungate del servizio per catastrofi naturali o per attacchi di tipo *Denial of Service*[18], sono alcune delle questioni che vengono discusse.

-*Incident Response* fornisce indicazioni sulle contromisure da adottare a seguito di attacchi alla sicurezza in un ambiente *cloud*.

1.5 Domini di sicurezza identificati da ENISA

L'Agenzia *European Network and Information Security Agency* (ENISA)[19] è un altro organismo con competenze specifiche su *network* e *informationsecurity*, creata al servizio della Comunità Europea, dei suoi stati membri e del settore privato. ENISA ha pubblicato il suo primo documento *Cloud computing Benefits, risks and recommendations for information security* nel Novembre 2009, con una ultima revisione nel Dicembre 2012 [20]. Il documento offre una definizione di *cloud computing* e ne evidenza i benefici chiave in termini di sicurezza e i principali rischi, classificandoli in tre categorie.

[18] *Denial of Service*, in "Wikipedia", (2013), http://it.wikipedia.org/wiki/Denial_of_service

[19] ENISA, http://www.enisa.europa.eu/

[20] ENISA, *Cloud Computing Benefits, risks and recommendations for information security*, rev. B, (2012)

-*Policy and organizational risks*:

1. Lock-in	2. Loss of governance	3. Suppy Chain Failure	4. Conflicts between customer	5. Social engineering attacks

Tabella 4: Rischi di natura non tecnica, derivanti dalla scelta di un *Cloud* Provider[21]

-*Technical risks* :

1. Resource exhaustion
2. Isolation failure
3. *Cloud* provider
4. Malicious insider
5. Management interface compromise
6. Intercepting data in transit
7. Insecure or ineffective deletion of data
8. Distributed denial of service
9. Economic denial of service
10. Compromise of Service Engine
11. Loss of Cryptographic Keys
12. Non *Cloud*-Specific Network-Related Technical Failures or Attacks
13. Loss of Backups
14. Natural disasters.

Tabella 5: Rischi di natura tecnica, associati al *Cloudcomputing*[22]

-*Legal risks* :

1. Subpoena and e-discovery	2. Risk from changes of jurisdiction	3. Data protection risks	4. Licensing Issues	5. Intellectual Property Issues.

Tabella 6: Rischi di natura legale, derivanti dall'utilizzo dei servizi di *Cloudcomputing*[23]

La categoria *Policy and organizational risks* copre cinque diversi problemi presenti in una piattaforma di *cloud computing*: il *lock-in* verte sulle problematiche di portabilità (migrazione) di dati e servizi tra *provider*, a seconda del modello di servizio adottato; a seguire la perdita di controllo del cliente nei confronti del *provider*, a cui delega gli aspetti di sicurezza; a sua volta il *provider* può garantire il servizio in *partnership* con altri *provider*,

[21] Fonte: ENISA
[22] Fonte: ENISA
[23] Fonte: ENISA

ma potrebbe verificarsi un disservizio a catena; la co-locazione di molti utenti provoca inevitabilmente conflitti per il *provider*, perché i requisiti di sicurezza nelle comunicazioni utente possono divergere tra loro; gli innumerevoli utenti del *cloud* e la facilità di interazione offrono, a colui il quale lancia un attacco, una grande superficie d'azione, esponendo le vittime all'arte della manipolazione finalizzata a divulgare informazioni confidenziali.

Le quattordici problematiche di natura tecnica cominciano con un elenco di rischi che possono dar luogo a minacce quali: la mancata disponibilità a causa dell'esaurimento delle risorse; un errore nell'isolamento delle VM; le minacce interne al *provider* stesso; i rischi legati ad attacchi di tipo *Denial of Service*; le minacce alla rete di connessione tra utente e *cloud*; la compromissione delle chiavi crittografiche; la perdita del *backup* a seguito di disastri naturali o meno.

Le cinque questioni legali trattano: citazioni che possono colpire il provider e lo stesso cliente, e, nel caso di sequestro dell'*hardware*, essendo questo condiviso, la probabile compromissione delle attività di altri utenti non coinvolti direttamente; il resto delle questioni giuridiche si concentra sul transito e la gestione dei dati in un altro Paese, con diversa giurisdizione, in cui risiede parte del *cloud*, con possibile cambio nella regolamentazione della protezione dei dati o rischio di perdere la proprietà intellettuale se non protetti da opportune clausole contrattuali.

2. Gestione della sicurezza nel *Cloud computing*

2.1 Obiettivi

L'architettura della sicurezza del *cloud* è efficace solo se vengono applicate le corrette e idonee difese, così come è stato osservato dall'analisi dei domini di sicurezza. La gestione della sicurezza ha come obiettivo quello di individuare i potenziali rischi e di affrontarli con gli idonei controlli. Questi controlli vengono impiegati per salvaguardare eventuali debolezze o criticità del sistema e ridurre così gli effetti di un possibile attacco.

Non solo l'infrastruttura di rete, ma in ottica virtualizzazione dei sistemi e servizi SaaS, la progettazione e la gestione della sicurezza devono essere

considerate durante il suo ciclo di sviluppo, al fine di ridurre la possibilità di attacco e conseguente perdita di dati[24].

Lo sviluppo di *software* cosiddetto sicuro[25] si basa sull'applicazione a monte dei principi di design del *software*. Questi principi costituiscono la base fondamentale per la *Software Assurance,* che il *Software Security Assurance Report*[26] identifica come punto di partenza affinché il *software* abbia delle proprietà tali da assicurare che continuerà a funzionare in modo affidabile, nonostante la presenza di difetti inseriti intenzionalmente. Detto in altri termini, durante i test tale *software* deve essere in grado di resistere alla maggior parte degli attacchi e di contenere i danni prodotti al fine di ripristinare, appena possibile, un livello normale di funzionamento dopo ogni attacco[27]. La *Software Assurance* ha tra i suoi requisiti quello di garantire confidenzialità, integrità, e disponibilità[28] e l'*Information Security* in accordo con lo standard ISO 7498-2, prodotto dall'*International Standards Organisation (ISO),* vi aggiunge identificazione e autenticazione, autorizzazione e non ripudio, al fine di minimizzare le minacce in un sistema informativo tradizionale[29]. Gli stessi principi, con i naturali adattamenti, possono essere estesi al *cloud computing.*

2.2 Principi di sicurezza delle informazioni

2.2.1 Confidenzialità

Il principio della confidenzialità si prefigge di assicurare che dati e risorse non siano esposti a soggetti non autorizzati. Una minaccia alla confiden-

[24] YI WEI, M. B. BLAKE, *Service-Oriented Computing and Cloud Computing - Challenges and Opportunities*, in Internet *Computing*, IEEE, 2010, vol. 14(6):72-75

[25] S. RICCETI, *La sicurezza delle applicazioni - dal modello tradizionale al cloud*, (2010), p.8, in https://www.securitysummit.it

[26] L. J. AGUILAR, *CLOUD COMPUTING Notes for a spanish cloud computing strategy*, in Spanish Institute of Strategic Studies' Magazine, 2012, p. 92

[27] *Information Assurance Technology Analysis Center* (IATAC), *Data and Analysis Center for Software* (DACS), *Software Security Assurance*, in State of-the-Art Report (SOAR), 2007, p. 20

[28] M. PAUL, *Assuring Software Security Through Testing*, in "isc2.org", whitepaper VII.

[29] ISO 7498-2 (*Information processing systems – Open systems interconnection – Basic Reference Model* – Part 2: *Security architecture*

zialità, dovuto a imperizia o attacco, mette a rischio la riservatezza delle informazioni, siano esse memorizzate, in fase di computazione, o trasferite in rete. Anche nel *cloud* si deve prevenire l'intenzionale o non autorizzata divulgazione di informazioni. Questo a causa di scarsa o inesistente cifratura della trasmissione durante i trasferimenti in rete, o mancata autenticazione presso il sistema remoto[30]. Anche una debole *policy* di sicurezza o un mancato controllo di configurazione possono inficiare la riservatezza. Una politica in tal senso definisce i requisiti per garantire la privacy dei dati, la *policy* dovrebbe specificare chi può scambiare informazioni e che tipo di dati possono essere scambiati. Oltre a varie contromisure che includono la cifratura, il rigoroso controllo d'accesso e una adeguata formazione del personale, spesso autore inconsapevole di minacce interne. Aspetti correlati comprendono il mantenimento dei diritti di proprietà intellettuale e l'anonimato[31]. Queste considerazioni dovrebbero tradursi in specifiche che soddisfino quali informazioni vengono fornite all'utente e ciò che l'utente può visualizzare, oltre alla creazione dell'identità personale di colui che accede[32].

2.2.2 Integrità

Il principio di integrità delle informazioni richiede che il dato, o in generale un oggetto, non sia compromesso durante la sua esistenza e che possa essere modificato solo dai soggetti autorizzati a farlo. Un sistema che risponde ai requisiti di integrità, garantirà, con un alto livello, che la risorsa resterà inalterata rispetto al suo stato originale, salvo modifiche da parte degli autorizzati. Naturalmente il rispetto del principio, come già osservato per la disponibilità, è valutato sia per le risorse memorizzate, sia per quelle processate, sia per quelle in transito su una rete. Infatti l'integrità dipende dalla confidenzialità, senza quest'ultima la prima non può essere garantita e viceversa.

---

[30] V. WINKLER, *Cloud Computing: Privacy, confidentiality and the cloud*, in "TechNet Magazine", 2013, http://technet.microsoft.com/en-us/magazine/dn235775.aspx

[31] P. T. JAEGER, J. LIN, J. M. GRIMES, *Cloud Computing and Information Policy: Computing in a Policy Cloud?* In Forthcoming in the Journal of Information Technology and Politics, 2008, vol. 5(3):269-283

[32] J. CHASE, P. JAIPURIA, *Managing Identity and Authorization for Community Clouds*, Technical Report CS-2012-08, Department of Computer Science, Duke University, 2012

In generale, le modifiche necessarie sui dati o risorse non devono essere operate da parte di persone o processi non autorizzati, così come al personale o a processi autorizzati deve essere impedito effettuare modifiche non autorizzate e, in entrambi i casi, si deve poter rilevare l'avvenuta alterazione di questi ultimi[33].

Una politica adeguata deve fornire i requisiti per garantire l'integrità evitando gli accessi non autorizzati, l'esecuzione di codice malevolo, gli errori nelle applicazioni e nel codice. Lo stesso dicasi per l'inserimento accidentale di dati non validi o l'alterazione a seguito di modifiche fuori controllo. Gli strumenti, atti ad assicurare l'integrità, includono robuste procedure di autenticazione, sistemi di rilevamento delle intrusioni in rete, controlli *software* e restrizioni sull'*input* nelle interfacce, l'uso della cifratura e di algoritmi di *hashing* per la validità. Questi ultimi calcolano una "impronta" digitale, c.d. *digest*, sulla base dei *bit* che compongono il dato, che viene analizzata alla ricerca di minime modifiche rispetto a quella originale. Un dato modificato fornisce un *digest* diverso e quindi segnala la tentata modifica. Tra gli strumenti indispensabili va altresì annoverata l'idonea formazione del personale[34].

2.2.3 Disponibilità

Il terzo principio è la disponibilità, la quale sancisce che ai soli soggetti autorizzati sia permesso l'accesso puntuale e ininterrotto alle informazioni. Pertanto, un sistema informativo mantiene un requisito di disponibilità se assicura, con un elevato livello, che dati e risorse siano accessibili solo agli autorizzati e senza interruzione, quindi prevenendo attacchi di tipo *Denial of Service* (DoS). L'infrastruttura di *cloud computing* deve garantire che le informazioni siano a disposizione dei soli utenti autorizzati quando necessario, anche in caso di spostamento dei dati verso un altro *provider*, evitando il *lock-in*. L'accesso sicuro e immediato a dati e risorse del *cloud*, anche da parte dello stesso *provider*,garantisce un accettabile livello di prestazioni, al

[33] P SINGHAL, *Data Security Models in Cloud Computing*, International Journal of Scientific & Engineering Research, 2013, vol. 4(6), pp. 789-793

[34] D.V. SANJITHA, M.HIMASWANTHI, T.V.N.SAI SINDHURA, K.V.V. SATYANARAYANA, *Dependable and Secure Storage Services in Cloud Computing*, in International Journal of *Computer* Trends and Technology (IJCTT), 2013, vol. 4(4)

fine di gestire eventuali interruzioni, fornire ridondanza e mantenere attivi i sistemi di *backup*[35].

Anche in questo caso le minacce alla disponibilità possono essere intenzionali o meno. Nel primo caso abbiamo già evidenziato che questo è l'obiettivo degli attacchi che rientrano nella categoria DoS. Nella seconda ipotesi, guasti ai sistemi fisici, errori nel *software*, cancellazioni accidentali da parte dell'utente e/o amministratore, *policy* o controlli inefficaci, possono causare la violazione di disponibilità.

Una politica efficace, finalizzata all'implementazione di idonee contromisure, impone di negare l'accesso non autorizzato alle risorse impiegando rigidi controlli d'accesso, prevenendo attacchi esterni (monitorando le prestazioni e il traffico di rete usando *firewall* e/o altri sistemi di protezione), guasti ai sistemi e disastri naturali[36], Un aspetto critico è dato dal fatto che la maggior parte dei tempi di inattività, causati dall'indisponibilità non sono pianificati e possono influenzare il *business* dell'organizzazione[37], per questo occorrono *policy* sulla ridondanza dei sistemi critici e sul mantenimento di sistemi di *backup*. La disponibilità, appare chiaro, è dipendente e strettamente legata alla confidenzialità e all'integrità. Se queste ultime dovessero venire meno, la disponibilità non potrà essere garantita.

2.2.4 Non ripudio

Nel *cloud computing* vi è il rischio che un provider possa confutare che una particolare azione o transazione, richiesta dall'utente, sia stata o meno eseguita. Naturalmente vale il viceversa per l'utente nel caso in cui imputi gli effetti di un'azione o evento al provider e quest'ultimo richieda per se una prova a sua discolpa. Il *non ripudio* sulla generazione di un evento o per la trasmissione dei dati, offre certezza che chi trasmette e chi riceve non possa negare di aver rispettivamente inviato e ricevuto i dati o condotto l'azione.

---

[35] S. PAGE, *Cloud Computing-Availability*, in " uwcisa.uwaterloo.ca", 2011, University of Waterloo, http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20*Cloud*%20*Computing*-Availability%20S%20Page.pdf

[36] A. MATHEW, *Security and privacy issues of cloud computing; solutions and secure framework*, in International Journal of Multidisciplinary Research, 2012, vol. 2(4), p.185

[37] T. ANDREI, *Cloud Computing* Challenges and Related Security Issues, 2009, http://www.cs.wustl.edu/~jain/cse571-09/ftp/*cloud*.pdf

Può essere ottenuto attraverso l'identificazione, l'autenticazione, e l'autorizzazione per mezzo di certificati digitali[38] e identificativi di sessione, seguiti da una fase di verifica e monitoraggio delle attività[39]

2.2.5 Identificazione e autenticazione

Durante la fase di identificazione il soggetto o entità fornisce un identificativo che può essere, per esempio, uno *UserID* che servirà per stabilire le responsabilità sulle azioni future compiute. Segue l'autenticazione con la verifica che l'identità fornita sia valida che, di solito, viene implementata attraverso la richiesta di una *password*[40].

L'autenticazione è normalmente basata su uno o più dei seguenti fattori:

Tipo 1 - Qualcosa che si conosce, come un PIN o una *password*;

Tipo 2 - Qualcosa che si possiede, come una tessera bancomat o *smart card*;

Tipo 3 – Qualcosa che si è, come una impronta digitale o la retina.

Un'autenticazione multi-fattore è più robusta rispetto all'utilizzo di una semplice *password* perché impiega più elementi per costituirla. Per esempio, allo sportello del bancomat ci autentichiamo con un qualcosa che possediamo (la *card*) e con qualcosa che conosciamo (il *pin*).[41]

A seconda del tipo di *cloud* e di modello di *deploy*, gli utenti sono individuati sulla base di strumenti di accesso *software* e/o hardware forniti loro dal provider del *cloud*.[42].

Una efficace politica in tal senso dovrebbe specificare quali siano questi strumenti e che caratteristiche tecnologiche presentino, così che ci sia la

---

[38] CLOUD SECURITY ALLIANCE, *Security as a Service: Defined Categories of Service*, 2011

[39] J. FENG, Y. CHEN, W. KU, P. LIU, *Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms*, in Parallel Processing Workshops (ICPPW), 2010 39th International Conference, 2010, pp. 251-258

[40] S. PAL, S. KHATUA, N. CHAKI, S. SANYAL, *A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security*, in Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research Article No. 76, 2011, p. 4

[41] M-M. D'COSTA-ALPHONSO, M. MICHAEL, *The adoption of single sign-on and multifactor authentication in organisations: a critical evaluation using TOE framework*, 2010, in Informing Science and Information Technology, vol. 7:161-190, p. 163-164

[42] B. MICHAEL, .G DINOLT, *Establishing Trust in Cloud Computing*, in IANewsletter, 2010, vol. 13(2), p. 7

massima trasparenza per l'utente che li debba utilizzare nel momento in cui viene richiesto un servizio *cloud*. La fase di autenticazione deve essere eseguita in modo sicuro, ad esempio, mediante l'uso di certificati a chiave pubblica che colleghino un utente ad una identità digitale[43].

2.2.6 Autorizzazione

L'autorizzazione si riferisce a diritti e privilegi, concessi a un utente o ad un processo, che consentono l'accesso ai servizi del *cloud*. È un importante requisito di sicurezza dal momento che viene impiegata per assicurare che sia mantenuta l'integrità delle informazioni. Infatti, una volta conclusa la fase di autenticazione, si deve affrontare quella di autorizzazione per consentire l'accesso alle risorse. In questa fase vengono stabiliti i livelli di privilegio che determinano le possibilità di azione di un utente[44].

Anche le *policy* di autorizzazione devono specificare quali strumenti impiegare per fornire il controllo degli accessi e come gestirli, per verificare che i privilegi siano assegnati correttamente agli utenti o ai processi durante la loro attività nel sistema *cloud*[45].

2.3 Verifiche e monitoraggio a garanzia della qualità dei servizi

Per la verifica dei sistemi di sicurezza implementati nel *cloud* si ricorre a processi di valutazione (*auditing)* e monitoraggio. Gli esiti possono essere valutati in termini di "fiducia" (*trust*) del cliente nei confronti di una terza parte (*provider*) che interviene nella catena della fornitura del servizio[46].

Un sistema di *audit* valuta la bontà di un aspetto di funzionamento o evento del sistema dopo la sua implementazione, identificando eventuali op-

---

[43] H. KHARCHE, D. S. CHOUHAN, *Building Trust in Cloud Using Public Key Infrastructure*, in International Journal of Advanced *Computer* Science and Applications, 2012, vol. 3(3), p. 27

[44] D. GOLLMANN, *Computer security*, in WIREs Computational Statistics, John Wiley & Sons, 2010, vol. 2:544-554, pp. 544-545

[45] A. VINCENT, *Identity and Access Management in Cloud Computing*: Part 2, in "cybersquared.com", 2010.

[46] K. M. KHAN, Q. MALLUHI, *Establishing Trust in Cloud Computing*, in IT Professional , 2010, vol. 12(5), pp. 20-27

portunità di miglioramento di questi processi, evitando così possibili costi futuri di reingegnerizzazione a seguito di revisione e il venir meno di accordi contrattuali che prevedano un determinato comportamento e/o livello di servizio differente. Il monitoraggio consente di vagliare l'attività utente o del *provider*. L'*auditing* può essere condotto da personale specializzato interno all'azienda o esterno, in questo ultimo caso come società indipendente di valutazione[47]. Ai *provider* di servizi *cloud* è richiesto di controllare e dimostrare la conformità delle azioni in corso, con le richieste contrattualizzate dal cliente e secondo la normativa in atto[48]. Una verifica indipendente della conformità di un'organizzazione, a seguito di *auditing*, è regolata da alcuni standard internazionali, che forniscono certificazioni in tal senso. Alcuni esempi sono: la serie di standard ISO/IEC 27000 per l'*information security*[49]; la *Statement on Standards for Attestation Engagements No. 16* (SSAE 16)[50], che definisce uno standard di attestazione delle verifiche indipendenti sul rispetto e l'efficacia delle attività di sicurezza e dei controlli sui dati trattati, sancito dall'istituto americano *American Institute of Certified Public Accountants* (AICPA), e che sostituisce, dal 2011, il precedente *Statement on Auditing Standards No. 70* (SAS 70).

2.4 Servizi *enterprise* nel *Cloud* federato

Fino a poco tempo fa lo sviluppo del *cloud computing* è stato contraddistinto dal costante aumento di centinaia di *provider* indipendenti ed eterogenei in limitate aeree geografiche, per lo più nei Paesi più avanzati, caratterizzati dall'offrire servizi appartenenti alle tre principali categorie (IaaS, PaaS, SaaS). Anche i grandi fornitori di servizi *cloud* hanno una limitata presenza

[47] I. GUL, A. UR REHMAN, M H. ISLAM, *Cloud Computing Security Auditing*, in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference, 2011, pp. 143-148

[48] C. ZHIXIONG, J, YOON, *IT Auditing to Assure a Secure Cloud Computing*, in Services (SERVICES-1), 2010 6th World Congress, 2010, pp. 253-259

[49] ISO, *ISO/IEC 27001:2005 information technology - security techniques - information security management systems - requirements*, in "iso.org", 2008, http://www.iso.org/iso /catalogue_detail?csnumber=42103

[50] AICPA, *Statements on Standards for Attestation Engagements - SSAE 16*, in "aicpa.org", 2012, http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx

fisica, con infrastrutture solamente nelle aree dove risulta più profittevole[51]. Lo scenario attuale e quello del prossimo futuro puntano entrambi ad avere sempre più interazione tra i diversi *cloud* esistenti che, pur mantenendo la loro indipendenza, cooperano e scambiano servizi tra loro, in un'ottica di un grande *cloud* federato[52]. Attualmente diversi grandi provider hanno già stabilito accordi per iniziare a fornire i loro servizi ad altri *cloud* provider. Per esempio, il progetto *open source* Eucalyptus[53] (con la sua piattaforma IaaS di *cloud* privato), offre ai suoi utenti compatibilità con le API della piattaforma *Amazon Web Services* (*cloud* pubblico IaaS), ottenendo in effetti un esempio di *cloud* ibrido. È anche vero che sperare di avere un unico grande *cloud* elastico, potendo condividere risorse di archiviazione e capacità di calcolo delle altre infrastrutture virtualizzate a seconda della domanda, non risulta facile a causa di meccanismi di privacy, affidabilità e tecnologie non ancora mature. Il tutto dovrebbe essere finalizzato al raggiungimento di un contesto di fiducia. Al momento sono allo studio diversi *framework* per lo sviluppo di un *intercloud*[54], orientati alla realizzazione di quanto sopradescritto.

2.5 Gestione delle identità digitali e modelli di autenticazione

Nel contesto digitale e *online* l'identità è definita come un insieme di informazioni corredate da attributi, che descrivono in modo univoco una persona o una cosa (a volte riferita come soggetto o entità), che fa richiesta di accedere a delle risorse e che contiene anche informazioni sulle relazioni

[51] D. BREDAHL , *Federation is the Future of the Cloud*, in "*Data Center Knowledge", 2012*,http://www.datacenterknowledge.com/archives/2012/09/17/federation-is-the-future-of-the-*cloud*/

[52] R. BUYYA, R. RANJAN, R. N. CALHEIROS, *InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services*, in Algorithms and Architectures for Parallel Processing - Lecture Notes in *Computer* Science, 2010, vol. 6081, pp 13-31

[53]*Eucalyptus 3 and Amazon Web Services (AWS)*, in "eucalyptus.com", 2012, http://www.eucalyptus.com/sites/all/files/ds-eucalyptus-aws.en.pdf

[54] Y. DEMCHENKO, C. NGO, C. DE LAAT, J. GARCIA-ESPIN, S. FIGUEROLA, J. RODRIGUEZ, L. CONTRERAS, G. LANDI, N. CIULLI, *Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand*, 2013

con altre entità[55]. Ogni attività *online* comporta l'interazione con un *provider* di servizi. Tali interazioni richiedono tipicamente che venga associata una identità digitale al soggetto e queste identità sono, per la maggior parte, memorizzate e gestite da ciascun *provider*[56]. Occorre quindi un'adeguata politica di gestione delle identità e degli accessi (*Identity and Access Management*), che descriva per ciascuna identità individuale come procedere all'identificazione del soggetto, alla sua autenticazione e autorizzazione.

Il processo di gestione prevede in generale che ci siano *Identity Provider* (IdP) che gestiscono le identità, *Service Provider* (SP), ovvero i fornitori di servizio per le funzionalità applicative (per esempio un provider SaaS), e gli utenti.[57] Nel caso delle entità persona, ciascun utente del *cloud* è associato ad una persona e, come osservato, sarà caratterizzato da un'identità e da una collezione di attributi che ne definiscono le proprietà (nel caso più semplice almeno due, UserID e *password*).[58]

Si hanno tre modelli di gestione delle identità: isolato; centralizzato; distribuito.

Il modello isolato è il più diffuso poiché è quello originario, dove ciascun utente possiede delle credenziali per ciascuno dei servizi a cui è registrato su diversi SP e ciascun servizio accede ad un archivio indipendente di credenziali gestito presso lo stesso SP di appartenenza. Le relazioni di fiducia con gli utenti descrivono come ciascun *provider* assicuri registrazione, meccanismi di autenticazione e gestione della singola identità, mentre l'utente deve garantirsi la gestione completa di tutte le identità dei vari servizi.[59]

---

[55] P. J. WINDLEY, *Digital Identity*, O'Reilly Media, Inc, 2008, pp. 8-9

[56] I. THOMAS, C. MEINEL, *An Identity Provider to manage Reliable Digital Identities for SOA and the Web*, in IDTRUST '10 Proceedings of the 9th Symposium on Identity and Trust on the Internet, 2010, pp. 26-36

[57] R. L. MORGAN, S. CANTOR, S. CARMODY, W. HOEHN, K. KLINGENSTEIN, *Federated Security:The Shibboleth Approach*, 2004, in EDUCAUSE Quarterly, vol. 27(4), pp. 12-17

[58] T. J. SMEDINGHOFF, *Introduction to Online Identity Management*, in "Uncitral", 2011, http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_Introduction_to_Identiy_Management.pdf

[59] A. JØSANG, J. FABRE, B. HAY, J. DALZIEL, S. POPE, *Trust requirements in identity management*, in Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44, pp. 99-108

Appare evidente come, nella situazione classica, a ciascuna entità possano quindi essere associate identità multiple su diversi SP. Questo comporta per l'entità persona, per l'organizzazione dove essa è impiegata e per il provider, una serie di oneri.

L'utente ha così troppi *set* di credenziali da ricordare. In secondo luogo, occorre implementare un archivio protetto per le credenziali e assicurarsi che il meccanismo di autenticazione funzioni in modo sicuro e corretto. Infine, il personale addetto deve offrire un supporto molto impegnativo, in quanto si trova a far fronte alla gestione delle nuove registrazioni, alla rimozione di utenti dal sistema e a casi in cui gli utenti perdono le loro credenziali e ne chiedono di nuove. Quindi la gestione delle identità si occupa di tutto il suo ciclo di vita, creazione, gestione e rimozione. In ultima istanza, purtroppo, gli utenti tendono a creare password deboli e facili da ricordare o a definire le stesse per diversi sistemi.

Tutti questi oneri possono essere minimizzati se si ricorre alla fiducia (*trust*), di una terza parte specializzata, ad un costo inferiore, per ottenere il servizio di gestione delle identità digitali di cui si ha bisogno. Normalmente l'utente o azienda di un *cloud* pubblico ripone la fiducia nel *cloud provider* da cui riceve i servizi. È ragionevole attendersi che a sua volta questo provider riponga la fiducia per la gestione delle identità in *outsourcing* presso un altro *provider* specializzato in tali servizi. Quest'ultimo *provider* (la terza parte), viene definito *Identity Provider* (IdP) e rientra negli altri due modelli di gestione.

Nel modello centralizzato, invece, è presente un solo IdP a cui fanno riferimento i diversi SP per validare le richieste di autenticazione giunte dall'utente. In questo caso è possibile abilitare il *Single Sign On* (SSO), che consente all'utente di utilizzare la stessa identità su più sessioni, in diverse applicazioni e su diversi SP da cui riceve servizi, poiché l'identificatore ad essa associato è unico e gestito dall'IdP, anch'esso unico (questa è una criticità perché rappresenta un unico punto di rottura). Di *default* si stabiliscono relazioni di fiducia tra i vari SP e l'IdP all'interno del dominio[60]. Per esten-

[60] R. WARSCHOFSKY, M. MENZEL, C. MEINEL, *Automated Security Service Orchestration for the Identity Management in Web Service based Systems*, in Web Services (ICWS), 2011 IEEE International Conference , 2011, pp.596-603

dere il concetto a relazioni interdominio dobbiamo ripensare il modello in ottica di federazione.

Infine, nel modello distribuito sono presenti diversi IdP e l'utente possiede diverse identità a lui riconducibili, su diversi domini della federazione[61].Quindi, in seguito, in una logica di federazione si possono collegare due o più di queste identità, relative allo stesso utente e con accordi di *trust* tra SP e IdP, e accedere ai diversi servizi della federazione con una unica identità, abilitando il SSO (un utente si autentica su un dominio e poi sarà in grado di accedere alle risorse di questo e di un secondo dominio federato). La gestione della federazione delle identità si occupa quindi di preservare le relazioni di fiducia che si stabiliscono tra diverse organizzazioni aderenti alla stessa federazione. Il modello si è sviluppato negli ultimi anni tramite diversi standard che abilitano lo scambio di informazioni utente tra gli elementi dei vari domini, tra i quali SAML, OpenID, OAuthe ciascuno può offrire alla federazione un servizio di autenticazione SSO. In questo modo ciascun SP ha la possibilità di verificare le identità gestite da altri IdP nella federazione[62]

Il *Security Assertion Markup Language* (SAML) è un *set open standard* di OASIS[63] di tipo "XML-*based*" per comunicare messaggi di autenticazione, autorizzazione e attributi dell'identità tra diversi domini della federazione, approvato nel 2002. Attualmente viene utilizzata la versione due, approvata nel 2005. Un IdP e un SP possono condividere attributi d'identità *web* in un messaggio SAML detto asserzione (o dichiarazione a seguito di richiesta), trasportato con HTTP. Le asserzioni non sono altro che documenti XML spediti da un IdP a un SP contenenti *info* di identificazione dell'utente che ha iniziato la procedura di richiesta SSO[64]. Possono essere di tre tipi: di

[61] Con il termine federazione, in linea con quanto già affermato in precedenza in tema di *cloud* federato, si intende l'associazione di organizzazioni che si uniscono per lo scambio di informazioni sui loro utenti e di risorse.

[62] Q. PHAM, A. MCCULLAGH, E. DAWSON, *Consistency of user attribute in federated systems,*in Trust, *Privacy* and Security in Digital Business , 2007, pp. 165-177

[63] OASIS, 2013, https://www.oasis-open.org/

[64] OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, in sstc-saml-tech-overview-2.0-draft-1, 2006, p. 5

autenticazione[65] se emessa per dichiarare l'identità; di autorizzazione[66] se dichiara che l'utente è stato autorizzato ad accedere a determinate risorse; di attributo[67] se specificano una serie di parametri dell'identità, per esempio il ruolo, l'*email* o il dipartimento di lavoro. Un classico scenario è quello che si presenta quando un utente vuole accedere ad un servizio presso un SP che però non gestisce le sue credenziali. Dalla pagina di login dell'SP, il *web browser* dell'utente sarà reindirizzato a quella dell'IdP tramite un messaggio SAML di richiesta autenticazione (che può essere anche cifrato e firmato digitalmente). L'IdP, che gestisce l'identità dell'utente, propone il login e una volta effettuato con successo crea un'asserzione o *token,* che dichiara la conferma dell'identità fornita e ridirige il *browser* alla pagina dell'SP. Quest'ultimo a sua volta verifica il *token* e ne estrae le informazioni che poi userà all'interno dei suoi sistemi. In questi passaggi le credenziali utente non sono mai transitate, vi è stata solo una conferma di fiducia tra SP e IdP.

Creato nel 2005, OpenID[68] rappresenta un altro standard aperto per l'identità federata. Consente ai suoi utilizzatori di usufruire delle funzionalità SSO, in un sito *web* che si affida, per la gestione delle identità, a un *provider* OpenID. Gli utenti scelgono il loro *provider* OpenID preferito (Google, Yahoo! e altri che hanno emesso OpenID per tutti i loro clienti) e usano i riferimenti del tipo *Uniform Resource Locator* (URL) per questi *account*, gli OpenID appunto, al fine di autenticarsi sui siti *web* che offrono tale servizio di accesso[69]. Ancora una volta gli SP non dovranno implementare un sistema di gestione delle identità e i loro utenti non dovranno creare un *account* per quello specifico *provider*. Grazie ad un protocollo di *discovery*, dato l'URL- utente, il *Service Provider* sarà in grado di risalire al *provider* OpenID e di reindirizzarvi il *browser*-utente mostrando il suo *form* di *login*. Una volta confermata l'autenticazione e autorizzato lo scambio tra SP e *pro-*

---

[65] *SAML Authentication*, in "oracle.com", 2011, http://docs.oracle.com/cd/E21455_01/ common/tutorials/authn_saml_assertion.html

[66] *SAML Authorization Assertion*, in "oracle.com", 2011, http://docs.oracle.com/cd/ E21455_01/common/tutorials/authz_saml_assertion.html

[67] *Retrieve Attribute from SAML Attribute Assertion*, in "oracle.com", 2011, http://docs.oracle.com/cd/E21455_01/common/tutorials/attributes_saml_assertion.html

[68] OPENID, 2013, http://openid.net

[69] T. ISLES, *How Does OpenID Work?*, in "My Tech Blathering", 2008, http://blog.tinisles.com/2008/02/how-does-openid-work/

vider OpenID, la *web application* usa le informazioni restituite per riconoscere l'utente e consentirgli l'accesso al servizio desiderato[70].

Infine, lo standard aperto OAuth [71]fornisce un metodo per gli utenti per concedere a terzi l'accesso alle loro risorse, proteggendo contemporaneamente le loro credenziali. La prima versione è stata rilasciata nel 2007 e nel 2012 la versione 2.0 del *framework* è stata ratificata dall'IETF [72]. L'ispirazione per OAuth, con l'avvento dei *social network* e delle applicazioni per il mobile, è stato quello di standardizzare il modo in cui gli utenti autorizzino un sito o applicazione (*client* nei ruoli definiti dallo standard) ad accedere ai dati del profilo utente registrato in un altro sito (il *server* di risorse), senza che il *client* debba chiedere all'utente di fornirgli le credenziali, per poi poter fare da se la chiamata all'API. In questo modo il *client* non dovrà richiedere al nuovo utente di registrarsi, ma potrà far usare al suo posto, per esempio, l'account di Facebook (*server* di autorizzazione), che a *login* avvenuto rilascerà un *token* di autorizzazione che consentirà al *client* di conoscere le informazioni del profilo utente (nome, foto, genere, elenco amici) ed integrarle nella nuova applicazione[73].

3. Analisi di vulnerabilità, minacce e rischi del *cloud computing*

Come è stato osservato in precedenza, il *cloud computing* aggiunge un ulteriore livello di rischio per il reparto IT, perché i servizi essenziali sono spesso affidati a soggetti terzi, il che rende più difficile mantenere la sicurezza dei dati e della privacy, la disponibilità del servizio e la conformità a regolamenti e standard. Le maggiori problematiche di sicurezza si articolano nei tre modelli di servizio (IaaS, PaaS, SaaS) e identificano le principali vulnerabilità riscontrate finora in questo tipo di sistemi e le più importanti minacce. Rischio, minaccia e vulnerabilità sono termini che molto spesso sono

[70] GOOGLE, *Federated Login for Google Account Users*, in "Google Accounts Authentication and Authorization", 2013, https://developers.google.com/accounts/docs/OpenID

[71] OAuth, 2013, http://oauth.net/

[72] IETF, *The OAuth 2.0 Authorization Framework*, in "Request for Comments: 6749", 2012, http://tools.ietf.org/html/rfc6749

[73] M. N. KO, G. P. CHEEK, M. SHEHAB, R SANDHU, *Social-networks connect services*, in *Computer*, 2010, vol. 43(8), pp. 37-43

utilizzati per rappresentare la stessa cosa. In realtà hanno differenti significati e sono in relazione tra loro. L'*International Organization for Standardization* (ISO), nelle linee guida per la gestione del rischio nel campo *dell'information security*, definisce il rischio come il potenziale che una data minaccia sfrutti le vulnerabilità di una o di un gruppo di attività, causando, di conseguenza, danni per l'organizzazione. Viene misurato come combinazione della probabilità del verificarsi di un evento e delle possibili conseguenze[74]. Quindi la vulnerabilità si riferisce ad una debolezza, riscontrata nel *software*/*hardware* o procedura, che permetta, per esempio, un accesso non autorizzato alle risorse del sistema. Laminaccia, una volta nota la vulnerabilità, è un potenziale attacco nel tentativo di arrecare danno o distruggere risorse. Il rischio rappresenta così la probabilità che una minaccia, sotto forma di attacco, ottenga il vantaggio sperato da una vulnerabilità e quale impatto abbia sul business aziendale.

3.1 Vulnerabilità nelle infrastrutture di virtualizzazione

Il *cloud computing* sfrutta diverse tecnologie oggi esistenti quali *Web* S*ervices*, *web browser* e la virtualizzazione, che contribuiscono alla sua evoluzione. Pertanto le vulnerabilità note e associate singolarmente a queste tecnologie e alle procedure riguardano anche il *cloud* e possono avere su di esso un impatto significativo. Di seguito vengono proposti alcuni possibili esempi.

In particolare, quando il si possono registrare delle vulnerabilità in relazione alle interfacce *software* e alle API. Da una parte il *cloud* mette a disposizione API per eseguire la maggior parte delle funzioni di gestione e consumo di risorse. Dall'altra, gli utenti usano i protocolli di comunicazione per i *Web Services*, tra i più popolari ricordiamo il SOAP[75]. La sicurezza del *cloud* dipende quindi dalla sicurezza di queste interfacce e protocolli e può venir meno a causa delle credenziali di accesso alle risorse. Altre vulnerabi-

[74] ISO/IEC, *Information technology -- Security techniques -- Information security risk management*, 27005:2011

[75] W. DAWOUD, I. TAKOUNA, C. MEINEL, *Infrastructure as a service security: Challenges and solutions*, in Informatics and Systems (INFOS), 2010 The 7th International Conference, 2010, pp. 1-8

lità sul *software* possono derivare da insufficienti controlli di autorizzazione sulle interfacce di programmazione, oppure da processi troppo semplici per la registrazione degli utenti, che non consentono un sufficiente *input* di dati per la fase di validazione dell'identità[76].

La vulnerabilità può riferirsi anche ai dati contenuti nel *cloud*. La condivisione delle risorse (*multi-tenancy*), può portare ad una coabitazione con dati di altri *tenant* sconosciuti (concorrenti o attaccanti),se questa viene progettata con una debole separazione tra le istanze dei diversi utenti[77]. Inoltre, i dati possono essere memorizzati o transitare in chiaro (senza cifratura) e in Paesi regolati da differenti leggi e regolamenti, per quanto riguarda contenuti e loro protezione. In questo modo le informazioni circa la loro attuale localizzazione nel *cloud* e quali operatori li stiano trattando possono risultare opache per l'utente[78]. Un'altra forma di vulnerabilità dei dati è rappresentata dall'impossibilità di cancellazione completa dei dati e delle eventuali copie a seguito di richiesta da parte dell'utente[79].

Con riferimento alle macchine virtuali, una possibile vulnerabilità può essere causata da errori individuati nelle memorie fisiche o nell'architettura del processore, abbinati a un insufficiente isolamento *software* tra le VM. Un'altra criticità che riguarda le VM risiede nell'uso incontrollato degli *snapshots*[80]. Infine, oltre ai casi sopracitati, potrebbe verificarsi una possibile migrazione incontrollata delle VM da un *server* a un altro *server*, per ragioni di *fault tolerance*, bilanciamento del carico, o per motivi di manutenzione.

Altro punto debole dei sistemi *cloud* è dato dalle immagini delle macchine virtuali. Infatti, le immagini *software* contengono i *file* di configurazione per creare le macchine virtuali e un pre-configurato sistema operativo. Molto spesso sono memorizzate in depositi pubblici fruibili dagli utenti. Un esempio è dato da Amazon con il suo *AWS Marketplace* propone uno *store*

---

[76] N.PHAPHOOM, X. WANG, P. ABRAHAMSSON, *Foundations and Technological Landscape of Cloud Computing*, in ISRN Software Engineering, 2013, Article ID 782174

[77] S. CARLIN, k. CURRAN, *Cloud Computing Security*, in International Journal of Ambient *Computing* and Intelligence, 2011, vol. 3(1), pp. 14-19

[78] P. T. JAEGER, J. LIN, J. M. GRIMES, S. N. SIMMONS, *Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing*, in First Monday, 2009, vol. 14(5)

[79] S. QAISAR, K. F. KHAWAJA, *Cloud Computing: Network/Security Threats And Countermeasures*, In Interdisciplinary Journal Of Contemporary Research In Business, 2012, Vol. 3(9)

[80] *Snapshots* = Preservano lo stato (accesa, spenta, sospesa) e i dati di una *virtual machine* (dischi, memorie, vNic) riferiti ad uno specifico istante

per i suoi utenti da dove prelevare oltre 500 *Amazon Machine Image* (AMI)[81]. Infine, un'altra criticità può essere rappresentata dalla propagazione di un'immagine priva di *patch* nell'ambiente di produzione.

Anche l'*Hypervisor* può essere fonte di vulnerabilità quando non configurato correttamente, poiché potrebbe tradursi in un unico punto critico per la sicurezza di tutti i componenti *software* da lui gestiti, indipendentemente dal grado di protezione delle singole VM. Allo stesso modo, la vulnerabilità dell'*Hypervisor* può essere data da una carenza nella tecnologia che implementa nell'isolamento logico delle VM, così come nei suoi deboli controlli di accesso e nella mancata applicazione di *patch*[82].

Nell'ambito di un sistema di macchine virtuali connesse da reti virtuali e collegate alla macchina *host* tramite *switch* virtuali, l'ultimo elemento di vulnerabilità è dato dalla maturità non ancora raggiunta dei sistemi di protezione virtualizzati, come i *virtual firewall*, comparata agli esistenti strumenti tradizionali per reti fisiche[83].

3.2 Minacce, rischi e contromisure

Come illustrato in precedenza, la *Cloud Security Alliance* rappresenta un punto di riferimento per l'industria del settore, proponendo standard e linee guida. CSA riconosce che una componente centrale della gestione del rischio nel *cloud computing* sia quello di comprendere la natura delle minacce alla sicurezza. Per questo con il report *The Notorious Nine*[84] presenta le principali minacce nel 2013. L'obiettivo dell'indagine è quella di fornire alle organizzazioni la comprensione delle minacce nel *cloud* al fine di adottare le

[81] *Amazon Machine Image* (AMI), in "Amazon Web Services", 2013, https://aws.amazon.com/marketplace/ref=mkt_ste_amis_redirect?b_k=291

[82] Virtualization special interest group PCI Security Standards Council, *Information Supplement: PCI Data Security Standard Virtualization Guidelines*, in "PCI Security Standards Council", 2011, https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

[83] T. T. BROOKS, C. CAICEDO, J. S. PARK, *Security Vulnerability Analysis in Virtualized Computing Environments*, in International Journal of Intelligent *Computing* Research (IJICR), 2012, vol. 3(1/2)

[84] R. LOS, D. GRAY, D. SHACKLEFORD, B. SULLIVAN, *The Notorious Nine: Cloud Computing Top Threats in 2013*, in "*Cloud* Security Alliance", 2013, https://*cloud*securityalliance.org/research/top-threats/

migliori decisioni di gestione del rischio. Nel 2010 un'analisi simile indicava ai primi tre posti l'abuso dei servizi *cloud*, le minacce contro interfacce e API non sicure e le minacce interne. Ora queste, benché ancora in elenco, sono scese di posizione (7, 4, 6, rispettivamente). Le seguenti minacce possono essere relazionate con le precedenti vulnerabilità, al fine di comprendere quanto affermato inizialmente, ovvero come una minaccia possa trarre vantaggio da una vulnerabilità per compromettere un sistema.

3.2.1 Violazione dei dati e integrità delle risorse

Quando più macchine virtuali appartenenti a utenti diversi (*tenant*), condividono la stessa macchina fisica, le vulnerabilità sui dati e sugli oggetti virtuali (VM, immagini e reti) in un sistema *multi-tenant* non progettato correttamente, possono essere sfruttate da un attaccante per accedere non solo ai dati dell'utente vittima, ma ai dati di tutti gli altri *tenant*, ponendo a rischio la confidenzialità. Ci sono diversi studi al riguardo che utilizzano tecniche sofisticate di *covert* e *side channels*[85][86].

Possibili contromisure possono essere la cifratura dei dati memorizzati, che aiuta a ridurre l'impatto di una eventuale violazione, ma che, in caso di perdita o compromissione delle chiavi, può comunque portare ad un'ennesima criticità o fare uso di firme digitali.

Anche un eventuale mancato controllo sull'integrità delle immagini messe a disposizione nei *repositories* pubblici può essere sfruttata per compromettere l'utilizzo delle macchine virtuali e costituire una criticità per tutti coloro che ne usufruiranno. Per esempio un attaccante con un *account* valido può depositarvi un'immagine con codice malevolo come un *trojan horse*, oppure potrebbe recuperare dei dati confidenziali (*password*, chiavi crittografiche) da immagini dismesse e non opportunamente "ripulite".

È necessario che le immagini dei sistemi operativi delle VM siano memorizzate localmente in un singolo *storage* logico o *library*, così da velocizzare i tempi di accesso in caso di ripristino e diminuire i tempi di disservizio.

---

[85] Z. WANG, R. B. LEE, *Covert and Side Channels due to Processor Architecture*, in Proceedings of the 22nd Annual *Computer* Security Applications Conference, 2006 pp.473-482

[86] Y. XU, M. BAILEY, F. JAHANIAN, K JOSHI, M. HILTUNEN, R. SCHLICHTING, *An Exploration of L2 Cache Covert Channels in Virtualized Environments*, in Proceedings of the 3rd ACM workshop on Cloud computing security workshop, 2011, pp. 29-40

Inoltre, non deve mai mancare un'adeguata protezione dall'accesso non autorizzato e una puntuale verifica della loro integrità mediante meccanismi di *checksums*, le cui informazioni devono risiedere separatamente dalla *library*.

Le minacce ai dati possono anche essere condotte tramite *network* dall'esterno nel momento in cui la rete virtuale è connessa alla rete fisica.

Gli utenti, per accedere in maniera sicura al *cloud*, hanno bisogno di utilizzare canali di comunicazione protetti per preservare privacy e integrità. Soluzioni di tunnel VPN o accessi remoti con SSH, tra *client* e *provider*, garantiscono, con efficaci algoritmi di cifratura, un'adeguata protezione sino all'accesso, ma non mettono al sicuro i percorsi interni al *cloud*. L'uso dello standard *WS-Security* all'interno, protegge a livello di messaggio SOAP le comunicazioni con i *Web Services*, ma in questo modo dovrà essere garantito il supporto degli standard in tutti i punti.

Le minacce dall'interno possono partire da una VM all'altra, se non vi è un'opportuna separazione tra le VM ospitate sullo stesso *host* fisico. Un attaccante può sfruttare la tecnica dell'*Address Resolution Protocol* (ARP) P*oisoning* per falsare la tabella ARP della VM vittima con uno *spoofing* di coppie fittizie di indirizzi MAC e IP (ponendo come MAC il proprio e come IP quello del *target*), reindirizzando il traffico, in uscita dalla VM e diretto all'IP del *target*, verso di sé e guadagnandone l'accesso (attacco di tipo *man-in-the-middle*)[87].

Pertanto la rete virtuale va adeguatamente protetta prendendo spunto dagli strumenti e dalle tecniche applicati alle reti fisiche e abilitando canali di comunicazione sicuri per mezzo della crittografia a chiave pubblica[88], contro il *network sniffing*.

Le VM sono tenute isolate dall'*hypervisor* non potendo leggere memoria, dati e usare le applicazioni di un'altra. Tuttavia sono ancora possibili accessi non autorizzati e *port scanning*.

Le contromisure risiedono nell'aggiungere una protezione di tipo firewall, *antivirus* e/o *anti-spyware* e *intrusion detection* ad alcune o tutte le VM, tenendo però in considerazione un possibile rallentamento nelle per-

[87] W. CHRISTIAN, C. MEINEL, *Practical Network Security Teaching in an Online Virtual Laboratory*, in Proc. 2011 Intl. Conference on Security & Management , 2011, CSREA Press, Las Vegas, Nevada, USA

[88] VMware, *Properly Configure VLANs*, in vSphere Security, 2012, http://pubs.vmware.com/rvsphere-51/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-51-security-guide.pdf

formance a causa dell'impiego di risorse extra per effettuare la scansione simultanea delle VM. Oppure il *firewall* potrebbe essere previsto solo tra due VM in particolare o tra la scheda di rete fisica del *server* e una VM.

In aggiunta è possibile segmentare la rete virtuale confinando il traffico in VLAN distinte tra gli *switch* virtuali o usare schede di rete fisiche per separare in maniera ancor più sicura le zone virtuali tra loro, aumentando i costi per dispositivi e cablaggio.

Un'altra possibile minaccia, nel caso in cui siano abilitate le VLAN su *switch* che supportano le VLAN native (trasportano traffico privo di *tag* identificativo della VLAN), potrebbe consistere nell'attacco *VLAN-hopping* che consente di raggiungere il *target* su una VLAN che normalmente non sarebbe accessibile per l'attaccante. Sfrutta la tecnica del *double tagging* per inserire nel *frame* inviato un doppio *tag*. Quello più esterno identifica la VLAN nativa, quello più interno la VLAN del target. Il primo *switch* incontrato dal *frame*, prima di inoltrarlo al successivo *switch*, elimina il *tag* esterno poiché sulla VLAN nativa devono essere convogliati *frame* senza *tag*, mostrando così il *tag* interno, che può essere letto e quindi accettato dal secondo *switch* e raggiungere il *target* su quella VLAN, dopo aver eliminato anche questo secondo *tag*[89].

Per il *VLAN-hopping* gli *switch* virtuali VMware non supportano la VLAN nativa, ad ogni modo la vulnerabilità può ancora essere sfruttata se sono presenti altri *switch* configurati per utilizzarla. È essenziale evitare,quindi, di utilizzare la VLAN nativa. Inoltre, è bene eliminarla da quelle consentite sui *link* di *trunk* o comunque sceglierne una che non sia realmente utilizzata nella rete.

3.2.2 Strategie per prevenire la perdita dei dati

La perdita definitiva dei dati personali, che mette a rischio la disponibilità, il non ripudio e la fiducia degli utenti nel *cloud*, può ricondursi a due ragioni, oltre a quella di un attacco intenzionale di tipo *Denial of Service* (DOS). Qualsiasi cancellazione accidentale ad opera del *provider* o in caso di catastrofe naturale.

---

[89] CISCO SYSTEMS, *Double-Encapsulated 802.1Q/Nested VLAN Attack*, in VLAN Security White Paper, http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_ paper09186a008013159f.shtml#wp39211

Anche un'azione di *rollback* che riconduce una VM a stati precedenti per mezzo dei vari *snapshot*, può esporla a vulnerabilità già risolte in passato e che possono portare a privazione di dati o ad un suo reset, all'insaputa dell'utente[90].

È possibile limitare la minaccia predisponendo una gestione delle attività di *backup* dei dati e delle immagini su siti remoti. Opportuni contratti di servizio potrebbero consentire la gestione dell'attività di *audit* finalizzata a registrare e notificare qualsiasi attività di eliminazione.

Anche l'utilizzo di strumenti di *Data Loss Prevention* (DLP) aiutano a prevenire la perdita di dati critici, identificando le informazioni sensibili per il loro contenuto, indipendentemente dalla loro posizione (in transito, sul *server*, sull'*end-point*) e verificando se siano o meno autorizzate a lasciare l'azienda(attacco interno)[91].

Diversi attacchi possono sfruttare le carenze tecnologiche nei *web browser* e nei *Web Services*, entrambi ampiamente coinvolti nell'accesso al *cloud*.

Un *Web Service* può essere attaccato tramite *XML Signature Element Wrapping* che sfrutta il fatto che questo comunica tramite messaggi SOAP scambiati con *http*. La sola specifica *XML Signature* non riesce, in una struttura del messaggio SOAP intercettata, a nascondere la posizione dei suoi elementi, consentendo all'attaccante di spostarli e di inserirne di nuovi al loro posto, mantenendo invariata la firma e quindi l'integrità.

Una contromisura da adottare per evitare le compromissioni sopradescritte, è quella di utilizzare certificati digitali (X.509) di fiducia e implementare *WS-security*, che definisce gli standard per garantire che le comunicazioni scambiate tramite messaggi SOAP siano sicure, in abbinamento con la specifica *XML Signature*.

Un *web browser* usa il protocollo TLS/SSL per cifrare le credenziali e autenticare l'utente in una comunicazione *point-to-point* tra il *client* e il *cloud*. Questo significa che la presenza di un dispositivo intermedio, per la

[90] T. RISTENPART, Virtual Security: Information Leakage in *Cloud*s and VM Reset Vulnerabilities, University of Wisconsin, http://www.zurich.ibm.com/~cca/csc2011/talks/ristenpart-invited-csc2011.pdf

[91] T, TOMOYOSHI, H. TSUDA, T. HASEBE, R. MASUOKA, *Data loss prevention technologies*, in Fujitsu Scientific and Technical Journal , 2010, vol. 46(1): 47-55

gestione del traffico tra i due end, implica la necessità di decifrare ed uno sniffing in quel punto (*man-in-the-middle*) potrebbe rivelare le credenziali.

Per protezione il *browser* dovrebbe implementare *WS-security* in abbinamento alla specifica *XML encryption* per una continua cifratura dei messaggi SOAP scambiati. In questo modo si ottiene una cifratura a livello di messaggio *end-to-end*, mitigando lo *sniffing*.

3.2.3 Il furto di identità attraverso *hijacking* di un *account* o servizio

L'attività di *Hijacking* (letteralmente "dirottamento"), rappresenta la presa di possesso di un account utente o la perdita di controllo di un servizio altrui. L'*account hijacking*[92] è una forma di furto di identità personale, spesso compiuto avvalendosi del *phishing* (ingannando l'utente sulla reale identità del *server* e convincendolo a fornire informazioni personali sensibili) o di tecniche di *hacking*. In questo modo è possibile spiare il traffico, manipolare dati, restituire false informazioni, scalare i privilegi e reindirizzare gli utenti del *cloud* verso siti illegittimi, con il rischio di compromettere la confidenzialità, l'integrità e la disponibilità dei servizi.

Lo *Hijacking* rappresenta una delle minacce più diffuse, perciò occorre proibire la condivisione di credenziali tra utenti e servizi e utilizzare tecniche robuste di autenticazione a due fattori (per esempio una password più un *token hardware*). È altresì indispensabile impiegare un monitoraggio preventivo per individuare attività sospette non autorizzate.

3.2.4 Minacce alla sicurezza nelle funzionalità applicative

Le minacce possono provenire da accesso anonimo e riuso di *token* o password, autenticazione in chiaro e carenza nelle autorizzazioni, limitata azione di monitoraggio e di *logging* delle attività.

Più in dettaglio, alcuni attacchi alle API prendono spunto dal classico attacco *SQL injection*[93].

---

[92] ACCOUNT HIJACKING, in "MySecureCyberspace", 2012, http://www.mysecurecyberspace.com/encyclopedia/index/account-hijacking.html

[93] *SQL INJECTION* = attacca le applicazioni *web* che fanno uso di un DB SQL occultando del codice malevolo tra le righe di una *query* SQL. Una volta eseguita l'istruzione si può arrivare ad avere accesso al sistema con massimi privilegi. Un controllo attento dei contenuti in *input* e la cifratura delle credenziali inviate consentono di mitigare il rischio.

Una variante può utilizzare il *submit* di un frammento di *script java-script* in un *form* di un *web forum*. Se il sistema non è in grado di intercettare lo *script*, ogni altro utente che leggerà il post avrà l'esecuzione dello *script* nel suo *web browser*, quindi lato *client*[94]. Rientra tra i *Cross-site scripting* (XSS) che sono ad oggi la forma più popolare di attacco contro i siti *web* dinamici.

Le cosiddette *API Keys* sono utilizzate dal *web* e dai servizi *cloud* per identificare ciascuna la propria applicazione client a cui è legata. Vengono richieste dalle API per accedere alle loro funzionalità, ma non dovrebbero essere utilizzate come meccanismo di autorizzazione utente per l'accesso all'API. Sfortunatamente invece diverse applicazioni affidano erroneamente alle *API Keys* questo significato, creando per l'attaccante un facile presupposto. Google e Yahoo sono stati tra i primi ad usarle, ma oramai con il Web 2.0 la debolezza delle *keys* è diventata rapidamente evidente, tale da ripiegare su sistemi alternativi per l'autenticazione delle applicazioni e degli utenti, tra cui *OAuth*, il *Security Assertion Markup Language* (SAML) e codici di autenticazione *hash-based* (HMAC).[95]

Queste interfacce devono essere progettate per proteggere sia dai tentativi accidentali sia da quelli intenzionali di aggirare la relativa *policy*. Il rischio della manomissione dei dati, il ripudio, la divulgazione di informazioni e la scalata di privilegi del sistema, dipendono anche dall'efficacia nel controllo e filtraggio dei contenuti malevoli ricevuti, da un robusto controllo di autenticazione e di accesso, dalla crittografia e dal monitoraggio delle attività.

3.2.5 Indisponibilità dei servizi attraverso attacchi *Denial of Service*

Questo tipo di attacco punta ad ottenere, da parte di un attaccante, o da un gruppo (in questo caso si parla di *Distributed Denial of Service*), la disponibilità per sé di tutte le risorse possibili del *target*, consumando potenza del processore, memoria, spazio disco o banda. Per esempio inondando il

[94] LAYER 7 TECHNOLOGIES, *Protecting Your APIs Against Attack & Hijack*, in "Layer 7 Technologies White Paper", 2012, http://www.layer7tech.com/resources/files/white_papers/Protecting%20Your%20APIs%20Against%20Attack%20and%20Hijack.pdf

[95] R. LEMOS, *Insecure API Implementations Threaten Cloud*, in "Dark Reading", 2013, http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550

target con un numero indefinito di pacchetti che non sarà in grado di gestire. In questo modo il sistema non potrà soddisfare qualsiasi altra richiesta proveniente da utenti legittimi. Il rischio è che venga meno la disponibilità dei dati per l'utente. L'attacco DoS si sta diffondendo sempre più tra gli ambienti virtualizzati, diventando popolare quanto in quelli reali, se non di più, per il fatto che le VM condividono le risorse dell'*host* che le ospita.

Gli attacchi DDoS possono essere condotti da un solo attaccante. In principio, con una fase di intrusione per mezzo di *trojan horse,* penetra, a loro insaputa, nelle macchine cosiddette *zombie* perché ignare di essere utilizzate, da lì a poco per un attacco simultaneo. Più avanti su queste macchine vengono istallati strumenti DDoS, che consentono il controllo remoto necessario per lanciare l'attacco verso un *target* comune. Così si amplifica l'effetto rispetto ad un semplice DoS[96].

Esempi di difesa contro gli attacchi *Denial of Service* possono essere quello di limitare, per gli utenti autenticati, l'uso delle risorse disponibili al minimo indispensabile nelle VM o sull'*host* fisico, stabilendo delle soglie oltre le quali si procede con l'eliminazione delle richieste in arrivo,oppure rafforzando i controlli d'accesso per tutti gli utenti non autenticati[97] e regolando i *timeout* di attesa delle risposte.

Un'ulteriore difesa può prevedere l'uso di *Intrusion Prevention and Detection System* (IPS/IDS) anche per gli ambienti virtualizzati, consentendo di rilevare le "*firme"* tipiche di un attacco (DoS o altri), o un comportamento del sistema che risulta essere anomalo, rispetto a quello normale con cui sono stati settati. Se posizionati *inline* con il traffico entrante da analizzare sono in modalità IPS, IDS. Se risultano posizionati *offline* rispetto al flusso, lavorando in modalità promiscua con l'apparato di rete con cui si interfacciano e da cui avranno una copia del traffico da analizzare. Il livello di protezione può essere sul perimetro della rete ("*network-based"*) o direttamente sull'*host*, fisico o virtuale ("*host-based"*). Snort[98] rappresenta un popolare progetto *open source* di *Network* IDS/IPS.

---

[96] M. LANDESMAN, *What is a DDoS attack?*, in "About.com", 2013, http://antivirus.about.com/od/whatisavirus/a/ddosattacks.htm

[97] OWASP, Application Denial of Service, in "owasp.org", 2010, https://www.owasp.org /index.php/Application_Denial_of_Service

[98] SNORT, http://www.snort.org/

3.2.6 Minacce interne e privilegi da non sottovalutare

I *cloud provider* difficilmente rivelano i loro *standard* e le loro politiche di assunzione del personale, quindi il rischio che l'attacco possa essere lanciato dall'interno dell'azienda fornitrice non può essere ignorato. Il Programma CERN[99] definisce una minaccia interna come quella condotta contro la confidenzialità, l'integrità e la disponibilità delle informazioni di un'organizzazione, da un impiegato o altra figura interna, che ha, o aveva, accesso a dati e sistemi aziendali e, abusando di questo privilegio, arreca danno[100]. Il danno potenziale potrebbe essere elevato se venisse sottovalutato il rischio di *spoofing*, manomissione e trafugamento dei dati. I sistemi che dipendono esclusivamente da un singolo *provider* per la sicurezza sono ad alto rischio. Anche se venisse implementata la crittografia, se le chiavi non vengono conservate con il cliente e sono solo disponibili al momento dell'uso, il sistema sarà ancora vulnerabile agli attacchi interni.

Possibili contromisure che riguardano il *provider* consistono nel rafforzare la valutazione dei propri afferenti interni. Parallelamente il cliente potrebbe richiedere sul contratto di servizio maggiori requisiti sul personale e una maggiore trasparenza sulle attività di gestione e sulle norme di sicurezza interna, così come le notifiche sulle eventuali violazioni alla sicurezza.

3.2.7 Abuso dei servizi *cloud*

I servizi *cloud* sono a disposizione di chiunque, anche di *hacker* che lecitamente affittano per un certo tempo la potenza di calcolo dei *server cloud*, ma solo per eseguire una serie di atti dannosi, come ad esempio il lancio di attacchi *Denial of Service* dall'interno, la distribuzione di *spam* e *malware*. I servizi *cloud* attraggono gli hacker perché trovano in questi un modo economico e conveniente per l'anonimato e per usare batterie di *server* che, per esempio, facilitano la loro opera di *crack* delle *password*.

---

[99] CERT, *The CERT Insider Threat Center*, in "cert.org", 2012, http://www.cert.org/insider-threat/index.cfm

[100] E. CHICKOWSKI, *Cloud's Privileged Identity Gap Intensifies Insider Threats*, in "Dark Reading", 2013, http://www.darkreading.com/vulnerabilities---threats/clouds-privileged-identity-gap-intensifies-insider-threats/d/d-id/1138974

I *provider* dovrebbero migliorare le loro *policy* di registrazione degli utenti per evitare l'anonimato e aumentare le attività di *audit* e monitoraggio interno, alla ricerca di attività sospette sulle loro infrastrutture.

3.2.8 Insufficiente "*due diligence*" nella valutazione dei rischi sul *cloud computing*

Due diligence[101] identifica il processo di analisi iniziale per una valutazione delle condizioni e di tutte le caratteristiche che occorrono per avviare un'attività di business, in questo caso nel *cloud computing*. I benefici del *cloud* quali la riduzione dei costi, l'efficienza, la maggiore sicurezza, possono attrarre alcuni aspiranti *provider*, ma non tutti sono sufficientemente attrezzati per valutarne i rischi[102]. Potrebbero non avere l'esperienza per comprendere i diversi servizi o applicazioni *cloud*, quali debbano essere le responsabilità operative in risposta agli incidenti, l'uso della crittografia e il monitoraggio della sicurezza. Per molti di loro potrebbe trattarsi di livelli sconosciuti di rischio non precedentemente considerati. Si possono creare false aspettative verso gli utenti quando non si conoscono del tutto le tecnologie e i problemi di design del *cloud*.

Per affrontare la minaccia, il *provider* deve comprendere i rischi che comporta l'adottare questo nuovo modello di tecnologia e disporre di risorse capaci ad affrontarla.

3.2.9 Minacce alle tecnologie condivise e *privilege escalation*

I *cloud provider* offrono i loro servizi in maniera scalabile condividendo infrastrutture, piattaforme e applicazioni. Tutti i modelli di servizio (IaaS, PaaS e SaaS), presentano questa caratteristica. Occorre allora un'adeguata strategia di difesa a tutti i livelli: elaborazione, memorizzazione, rete, applicazione ed attuazione della sicurezza per l'utente, insieme alle attività di *audit* e monitoraggio. Un guasto o un attacco accidentale può avere effetti sull'intero *cloud* se il *provider* non gestisce correttamente i requisiti di isolamento delle tecnologie condivise. Singoli *tenant* non devono impattare sul-

[101] *Due diligence*, in "Wikipedia", 2013, http://it.wikipedia.org/wiki/Due_diligence

[102] SAN ANTONIO EXPRESS-NEWS, *Perfecting the Unknown: Cloud Computing*, in "mySA.com", 2012, http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-*Cloud-Computing*-4157844.php

le *performance* degli altri sullo stesso *cloud* e non devono avere accesso ai loro dati.

Spesso i componenti di base che compongono l'infrastruttura fisica non sono stati progettati per permettere un efficace isolamento, come richiesto da una architettura *multi-tenancy*. Allora nell'ambiente virtualizzato spetterà all'*hypervisor* mediare l'accesso tra i sistemi operativi delle VM e le risorse fisiche di calcolo. Appare evidente che una compromissione della sicurezza dell'*hypervisor* espone a forti rischi più di un utente del *cloud*.Come è stato osservato tra le vulnerabilità, la minaccia potrebbe arrivare da un *hypervisor* non "patchato", spesso appena acquistato e non correttamente configurato

Un attacco che ha avuto rapida diffusione è quello che rientra nella categoria degli *escape*, in questo caso di *escape to hypervisor*[103], dove una VM compromessa consente all'attaccante di "evadere" dalla sua istanza in cui è stata giustamente confinata e di passare al livello successivo scalando privilegi locali e potendo eseguire del codice nel contesto *hypervisor*[104].

[103] M. J. SCHWARTZ, *New Virtualization Vulnerability Allows Escape To Hypervisor Attacks*, in "InformationWeek", 2012, http://www.darkreading.com/risk-management/new-virtualization-vulnerability-allows-escape-to-hypervisor-attacks/d/d-id/1104823

[104] J. GRUSKOVNJAK, *Advanced Exploitation of Xen Hypervisor Sysret VM Escape Vulnerability*, in "VUPEN Security", 2012, http://www.vupen.com/blog/20120904.Advanced_ Exploitation_of_Xen_Sysret_VM_Escape_CVE-2012-0217.php

PARTE TERZA - DALL'*E-GOVERNMENT* ALL'*E-HEALTH*

1. Aspetti generali

Prima di analizzare gli aspetti peculiari delle applicazioni del *Cloud Computing* nella sanità è opportuno evidenziare come tale tecnologia si stia diffondendo all'interno della Pubblica Amministrazione[1] da una parte come nuovo modello flessibile ed economico di fornitura di servizi *ICT*, dall'altra come nuovo metodo di progettazione, realizzazione e gestione di sistemi informativi che permetterà di migliorare il rapporto tra Stato e cittadini. L'adozione di soluzioni *cloud* consente il risparmio e la razionalizzazione delle risorse informatiche, facilitando il conseguimento degli obiettivi di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza dell'agire amministrativo[2].

---

[1] V., fra gli altri, A. LISI - S. UNGARO, *Cloud e PA: sarà più facile andare 'sulle nuvole'*, in Guida al pubblico impiego, 2013, I-II, 53; A. LISI - S. UNGARO, *Cloud & PA: nuovi profili di responsabilità*, in Guida al pubblico impiego, 2012, V, 29; A. LISI - S. UNGARO, *Cloud: vanno indicati ruoli e responsabilità*, in Guida al pubblico impiego, 2012, X, 59; M. PÒ, *Dal Cloud computing nuove opportunità per la Sanità*, in Guida al pubblico impiego, 2012, V, 30; A. OSNAGHI, *Pubblica amministrazione che si trasforma: «Cloud Computing», federalismo, interoperabilità*, in Amministrare, 2013, I, 59; D. GLORIO, *Il Cloud Computing nella P.A. e nei servizi demografici*, Lo Stato civile italiano, 2013, III, 37, e C. FLICK - V. AMBRIOLA, *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in Federalismi.it, 2013, VI.

[2] Il ricorso a soluzioni di tipo *cloud computing* da parte della Pubblica Amministrazione non è un fenomeno soltanto italiano, bensì di rilevanza Europea. Tra i documenti strategici e i programmi più rilevanti elaborati dall'Unione Europea è doveroso il riferimento alla "*Digital Agenda for Europe, EU Cloud Initiative, e-Government Action Plan 2011 – 2015*" e al "*Programma ISA, 7° programma quadro di ricerca, programma CIP – ICT PSP*", i quali si occupano in modo ampio delle tematiche legate all'adozione di tali tecnologie. Nello stesso verso anche il "Contributo all'analisi annuale della crescita 2014" (Rel. 13-11-2013, Analisi dei progressi compiuti e degli ostacoli ancora esistenti negli Stati Membri - Contributo all'analisi annuale della crescita 2014, COM/ 2013/785 final), presentato dalla Commissione Europea, che, nell'occasione, considera l'*ICT* come un'importante leva per la riforma e il risanamento delle amministrazioni. Un particolare riferimento, in tal senso, è proprio rivolto al *cloud computing* (a condizione che venga offerto sotto forma di servizio aperto), che è indicato come tecnologia su cui occorre investire per promuovere lo sviluppo delle infrastrutture di servizi digitali e per stimolare la domanda (Rel. 2013/785, § 2.5).

In tale direzione, il 10 luglio 2012, l'Agenzia per l'Italia Digitale[3] (già DigitPA) ha deliberato le "*Raccomandazioni e proposte sull'utilizzo del* cloud *computing nella Pubblica Amministrazione*"[4]. Il documento: "*da una parte raccoglie considerazioni e proposte rilevanti ai fini dell'adozione del cloud computing da parte della pubblica amministrazione in Italia. Dall'altra […] offrire strumenti utili a questo scopo privilegiando un approccio che oltre a proporsi con finalità di razionalizzazione e di risparmio miri anche a promuovere un'organizzazione innovativa dei servizi pubblici* online *che le soluzioni tecnologiche e operative del* cloud *rendono possibile*".

Pochi mesi dopo anche il Codice dell'Amministrazione Digitale (qui di seguito "CAD") è stato novellato, all'art. 68, co. 1, lett. d), con l'inclusione del *cloud computing* quale soluzione adottabile dalla Pubblica Amministrazione nella scelta dei servizi informatici[5].

È proprio con l'entrata in vigore del CAD che si è data una prima forte spinta al processo di digitalizzazione della Pubblica Amministrazione: fe-

---

[3] L'Agenzia per l'Italia Digitale è stata istituita con il Decreto legge n. 83, convertito nella legge n. 134/2012. La medesima fonte ha soppresso il Dipartimento Digitalizzazione e Innovazione della Presidenza del Consiglio, l'Agenzia per la diffusione delle tecnologie per l'innovazione, DigitPA, l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti. Le funzioni prima esercitate dai suddetti Enti, oggi sono tutte di competenza dell'Agenzia, oltre alle funzioni che le sono state attribuite con il Decreto Legge n. 179, convertito nella legge n. 221 del 2012.

[4] Il documento, nella sua ultima versione (2.0), è consultabile al seguente link: http://www.agid.gov.it/sites/default/files/documenti_indirizzo/raccomandazioni_cloud_e_pa_-_2.0_0.pdf . Sulla definizione di *cloud* fornita dal *National Institute of Standards and technology* (NIST) americano, presente anche nel report del 2010 dal titolo "*the future of Cloud Computing*" (redatto da un gruppo di esperti riuniti dalla Commissione europea) si tornerà nella parte quarta del presente lavoro.

[5] Si tratta della modifica al d.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) introdotta dal c.d. decreto crescita 2.0 (d.l. 18-10-2012 n. 179 conv. in l. 17-12-2012 n. 221), in base al quale oggi "*le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato: a) software sviluppato per conto della pubblica amministrazione; b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione; c) software libero o a codice sorgente aperto; d) software fruibile in modalità cloud computing; e) software di tipo proprietario mediante ricorso a licenza d'uso; f) software combinazione delle precedenti soluzioni*".

nomeno meglio conosciuto come *e-government* il cui obiettivo principale è quello di migliorare la capacità e l'efficienza dei servizi pubblici, attraverso l'uso delle nuove tecnologie, sia nei rapporti tra Pubblica Amministrazione e cittadini, sia tra le stesse Amministrazioni.

In tale direzione, l'art. 2 del CAD impone alle Amministrazioni (Stato, regioni e autonomie locali) di assicurare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale, attraverso l'adozione di appropriate tecnologie dell'informazione e della comunicazione. Inoltre, per le stesse Pubbliche Amministrazioni è previsto l'obbligo di garantire la consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni. Il *cloud computing* rappresenta una soluzione pienamente in linea con gli obiettivi qui descritti, inserendosi coerentemente all'interno di queste dinamiche di ammodernamento della Pubblica Amministrazione.

Si pensi, a tal proposito, facendo riferimento ai numerosi adempimenti imposti alla P.A., a quelli previsti dall'art. 50-*bis* del CAD (continuità operativa e *disaster recovery*), ovvero all'obbligo di digitalizzazione dei dati e documenti. Ebbene, spesso le singole Amministrazioni non dispongono di adeguate risorse *hardware* e *software* idonee ad assolvere tali obblighi e il *cloud computing*, nelle sue diverse applicazioni (IaaS/Paas/SaaS, privato/pubblico/ di comunità/ibrido), potrebbe rappresentare una valida soluzione in tal senso,in grado di consentire in modo efficiente, sia in termini di costi che di tempi, lo svolgimento di attività complesse. Uno dei tanti esempi è rappresentato dalla possibilità di accesso ai servizi direttamente dal portale *web*, sfruttando la caratteristica di *self-provisioning*[6] dei sistemi *cloud*, che è in grado di ridurre gli sprechi ed implementare rapidamente nuovi servizi senza affrontare sovraccarichi burocratici e amministrativi.

Nella medesima direzione, merita di essere citato in questa sede il Decreto Direttoriale del MIUR, n. 84/Ric. del 2 marzo 2012, intitolato "*Smart Cities and Communities and Social Innovation*", nel quale sono enunciate

[6] Col termine "*provisioning*", nelle telecomunicazioni si indica il processo di fornitura di infrastrutture informatiche, quali software, hardware e cablaggi. Il "*self-provisioning*" individua quella caratteristica del Cloud Computing, introdotta dal NIST (*National Institute of Standards and Technology*), che permette agli utenti di scegliere o di abbandonare i servizi Cloud, in modo autonomo senza richiedere particolare assistenza qualificata.

cinque azioni integrate per la società dell'informazione, fra cui "*Cloud computing technologies per smart government*", finalizzata a "*sostenere l'innovazione dei servizi al pubblico, con particolare riguardo al settore* e-Government*, e alle imprese, con particolare riferimento alle PMI, mediante lo sviluppo di prototipi funzionanti che contribuiscano ad adottare e diffondere piattaforme cloud e le relative applicazioni e servizi. Le nuove tecnologie dovranno essere in grado di migliorare la qualità e l'accessibilità dei servizi, garantire elevati standard di interoperabilità tra sistemi "cloud" differenti, promuovere implementazioni di riferimento basate su soluzioni open source, ridurre i costi di adozione da parte delle imprese di nuove tecnologie ICT, incrementando il ritorno degli investimenti e riducendo il «*time to market*» *dei loro prodotti e servizi.* "[7].

Il miglioramento della qualità e dell'accessibilità ai servizi passa attraverso soluzioni di tipo *cloud* integrate con l'adozione di sistemi *open source*, un binomio sempre più utilizzato per garantire nel contempo la riduzione dei costi e l'efficienza del mercato.

Le soluzioni di *e-government* sono state oggetto di dibattito anche a livello europeo. In particolare, nella risoluzione del Parlamento Europeo n. 2011/2178 intitolata "*Risoluzione del Parlamento europeo del 20 aprile 2012 sull'e-Government come elemento trainante di un mercato unico digitale competitivo*", al considerando "G" il *cloud computing* è inquadrato come "*uno strumento economico ed ecologico che permette di migliorare le prestazioni informatiche delle imprese pubbliche e private nonché di ridurre i costi di elaborazione e limitare quelli di archiviazione*". Dinnanzi a tali vantaggi, nella sua risoluzione il Parlamento Europeo non esitava ad evidenziare l'insufficiente sicurezza della connessione tra l'utente e il *server cloud* che comporta "*una certa perdita di controllo da parte dell'utente*".

Il legislatore europeo rilevava, altresì, che il *cloud computing*, a condizione che fosse tecnicamente affidabile e resistente, consentiva l'accesso a un gruppo condiviso di risorse informatiche che possono essere rapidamente ritrasmesse con uno sforzo minimo di gestione e una minima interazione del fornitore dei servizi, e che l'efficacia dello stesso risiede nella sua flessibilità, nell'aumento di produttività che comporta e nel suo contributo alla salvaguardia dell'ambiente.

[7] Art. 2.

Quanto alla digitalizzazione della pubblica amministrazione, il Parlamento sottolineava come le soluzioni di *e-Government*, riducendo i costi e gli oneri amministrativi, aumentando la produttività, l'efficienza, la competitività, la trasparenza, l'apertura, l'efficacia della politica, l'accessibilità e la razionalizzazione delle procedure, fossero particolarmente vantaggiose per i cittadini e gli imprenditori dell'UE, soprattutto per le PMI, che in quel momento si trovassero spesso ad affrontare barriere insormontabili nell'effettuare operazioni transfrontaliere all'interno dell'UE.

Infine, in un passaggio fondamentale della risoluzione, si evidenziava come l'incremento di soluzioni di *cloud computing* richiedesse il monitoraggio della delocalizzazione delle risorse informatiche e il controllo rigoroso dell'accesso ai *server* e ai dati, al fine di evitare qualsiasi utilizzo commerciale non autorizzato da parte di terzi. Le soluzioni a tali questioni, proseguiva il Parlamento, dovrebbero essere affrontate nel quadro della riforma delle norme UE in materia di protezione dei dati proposta dalla Commissione[8].

Un importante contributo alla diffusione del *cloud* nell'ambito delle pubbliche amministrazioni è dato dalle singole regioni, certamente più sensibili rispetto al legislatore nazionale ed europeo, viste le grosse voci di spesa nel bilancio pubblico e alla luce del potenziale risparmio economico offerto dalle nuove soluzioni *ICT*.

Un brillante esempio di normativa regionale di settore è offerto dalla Regione Puglia con la l.r. 24 luglio 2012, n. 20 recante "*Norme sul software libero, accessibilità di dati e documenti e hardware documentato*". La legge definisce il *cloud computing* come "*la modalità attraverso la quale è possibile distribuire risorse di calcolo, archiviazione, software e umane per diversi utilizzatori e scopi*"[9]e stabilisce che la Regione "*promuove una Comunità di pratica, aperta alle università e al partenariato economico e sociale, che favorisca lo sviluppo della digitalizzazione attraverso l'uso delle tecno-*

[8] Oggi il Regolamento europeo sulla protezione dei dati personali è realtà. Al tempo della risoluzione in commento il riferimento era alla procedura legislativa ordinaria n. 2012/0011/COD, con la quale il 25 gennaio 2012 la Commissione Europea trasmise la prima bozza contenente la "*Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati)*".

[9] Art. 3, lett. p), l.r. 24 luglio 2012, n. 20

*logie dell'informazione e della comunicazione in tutte le attività, al fine di superare le barriere interne all'introduzione dell'*e-business*, nelle imprese e nelle amministrazioni pubbliche*"[10]. Tale Comunità ha il compito di promuovere lo studio di fattibilità di sistemi *Cloud Computing* per la Pubblica Amministrazione tali da permettere la distribuzione di risorse di calcolo, archiviazione, *software* e umane per diversi utilizzatori e scopi.

Un altro settore in cui le soluzioni basate sulle tecnologie *cloud* consentono di apportare notevoli benefici è il mondo dell'istruzione scolastica, nell'ambito del fenomeno cosiddetto "*e-School*". A tal proposito è doveroso far riferimento alla Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni del 25 settembre 2013, n. 654, dal titolo "*Aprire l'istruzione: tecniche innovative di insegnamento e di apprendimento per tutti grazie alle nuove tecnologie e alle risorse didattiche aperte*". Con la Comunicazione si definisce un'agenda europea per la promozione di modalità di apprendimento e insegnamento innovative e di qualità attraverso le nuove tecnologie e i contenuti digitali, in linea con la strategia "Europa 2020"[11].

Per quanto concerne il *cloud computing*, la Commissione rileva che mentre a livello mondiale gli investimenti nella banda larga e nell'imprenditorialità consentono di creare notevoli opportunità commerciali, il potenziale economico dei *software* e dei contenuti didattici in Europa rimane in ampia misura inutilizzato. Per queste ragioni, secondo la Commissione "gli sviluppi nelle tecnologie e nei giochi *cloud*, la personalizzazione dell'apprendimento e i dispositivi mobili daranno impulso alla crescita nel mercato delle

[10] Art. 17, l.r. 24 luglio 2012, n. 20

[11] Com. 3-3-2010, "*Europa 2020. Una strategia per una crescita intelligente,sostenibile e inclusiva*", COM/2010/2020 final. Come ricorda anche la Corte Costituzionale, Sent. 27 giugno 2012, n. 163, l'Agenda digitale europea è stata qualificata dalla Commissione europea una delle sette iniziative "faro" della strategia Europa 2020, volta, ad un tempo, a stimolare la crescita economica e la competitività e ad offrire ai cittadini una migliore qualità della vita sotto forma di assistenza sanitaria migliore, trasporti più sicuri ed efficienti, ambiente più pulito, nuove possibilità di comunicazione e accesso più agevole ai servizi pubblici ed ai contenuti culturali. La strategia "Europa 2020" è stata anche richiamata più volte dalla Corte di Giustizia Europea, Sent. 20 gugno 2013 - C-20/12, Elodie Giersch e altri c. État du Grand-Duché de Luxembourg, e da ultimo dalla Sent. 15 ottobre 2014 – C-65/13, Parlamento europeo contro Commissione europea. In dottrina, per tutti, v. E. BATTELLI, *Il nuovo Diritto europeo dei contratti nell'ambito della Strategia "Europa 2020"*, Contratti, 2011, XI, 1065

tecnologie didattiche". Nell'ambito delle iniziative nazionali in materia di *e-School* si segnala l'accordo Stato-Regioni concernente la diffusione nelle scuole di ogni ordine e grado dei progetti e delle azioni di innovazione didattica[12]. Con l'accordo sono stati istituiti sei gruppi di lavoro interministeriali con il compito di attuare l'Agenda Digitale Italiana (in attuazione dell'Agenda Europea) e, in particolare, il gruppo "Competenze digitali" che, sotto il coordinamento del Ministero dell'Istruzione, dell'Università e della Ricerca, ha l'obiettivo di favorire l'adozione di soluzioni di *cloud computing*, per garantire un utilizzo flessibile e ottimale di risorse ed offrire a docenti e studenti aree riservate, aree servizi e *repository* di contenuti digitali. Nell'accordo il Ministero si è impegnato a mettere a disposizione delle scuole le soluzioni *di cloud computing* e i *repository* di contenuti digitali che saranno realizzati all'interno dell'Agenda digitale italiana.

Nell'ambito delle iniziative regionali volte alla diffusione e all'adozione di soluzioni di *cloud computing*, meritano di essere citate la regione Toscana, con la Del. G. Reg. 21 gennaio 2013 n. 40[13], e la regione Campania, con la Del. G. Reg. 25 novembre 2013 n. 501 concernente uno "*schema di protocollo di intesa tra regione Campania e poste italiane s.p.a.*"[14]. Nell'ambito della *e-School*, la regione Marche ha adottato la Del. G. Reg. 3 settembre 2012 n. 1259, recante "*Attuazione dei progetti e delle azioni di innovazione didattica negli Istituti scolastici marchigiani*" con la quale si è inteso dare concreta applicazione agli obiettivi stabiliti nell'accordo Stato-Regioni del 2012, attraverso la messa a disposizione delle infrastrutture *ICT* regionali quali la piattaforma TRIO, il sistema di *cloud computing* MCloud, il sistema di autenticazione federata FedCohesion e il polo di conservazione Marche DigiP.

---

[12] Acc. 25 luglio 2012, n. 118/CSR,

[13] La delibera riguarda l'"*Approvazione dello schema di accordo per lo sviluppo di azioni per la promozione del "Villaggio Digitale*" in cui, anche attraverso soluzioni *cloud*, si prevede una diffusione dei servizi on line della PA e dei servizi per l'Amministrazione digitale sviluppati sia da Regione Toscana che dagli Enti del territorio, da rendere disponibili, in una logica di condivisione, tramite un'unica piattaforma, messa a disposizione da Regione Toscana, rivolta a cittadini, associazioni e imprese, con sistema di autenticazione forte ed unificata tramite CNS.

[14] Tra i punti più significativi, le amministrazioni si impegnano a collaborare al fine di potenziare le infrastrutture tecnologiche per l'erogazione di servizi ai cittadini ed alle imprese attraverso servizi *Cloud* e *Disaster Recovery*.

1.1 Breve panoramica delle iniziative *Cloud* nella PA Italiana

Come si è visto, la Pubblica Amministrazione italiana si è dimostrata sensibile verso le innovazioni e le soluzioni in *Cloud Computing*. In questa sezione viene fornita una breve panoramica relativa ad alcune tra le più significative iniziative.

Assinter

L'Associazione delle Società per l'Innovazione Tecnologica nelle Regioni (Assinter) riunisce aziende ed enti locali in diversi progetti di informatizzazione delle pubbliche amministrazioni e, da qualche anno, sta portando avanti un progetto teso ad accompagnare le Regioni verso un'evoluzione *Cloud* in un ottica di cooperazione e condivisione. L'Emilia Romagna e il Trentino sono tra le Regioni capofila del progetto, le quali sono già dotate di un'infrastruttura adeguata in grado di fornire servizi verso altri enti e cittadini attraverso soluzioni *cloud* di tipo *as a Service*, nel rispetto dei principi del riuso.

L'obiettivo dei progetti Assinter è quello di mantenere la proprietà dei Data Center affinché le P.A. possano continuare a presidiare e controllare le risorse anche in un'ottica di maggiore tutela dei dati personali trattati e conservati nei sistemi *cloud*.

Azienda Ospedaliero Universitaria Ospedali Riuniti di Ancona

Attualmente l'infrastruttura dell'ente, composta da oltre 80 macchine virtuali, è collocata in ambiente *private cloud* attraverso l'adozione di tecnologie *open source* basate sul *tool* di gestione, sviluppato da Google, Ganeti. Inoltre, è stato avviato anche un progetto di architettura di *storage cloud* ibrido. Questo servizio è acquistato dall'esterno ed integrato su un'infrastruttura *open stack* fornita dalla Regione. L'architettura è in fase di studio e prevede la possibilità di accedere all'occorrenza a macchine virtuali su *silos*. L'adozione di Ganeti consente di abbassare il livello di complessità dell'infrastruttura e, allo stesso tempo, di mantenere i benefici di *open stack*. Rispetto ad altri enti sanitari, l'AOU di Ancona è una precorritrice assoluta nell'adozione di tecnologie in *cloud*, avendo adottato tali soluzioni già a par-

tire dal 2011. Attualmente anche la gestione dei respiratori si basa su una sistema in *cloud*.

Queste infrastrutture, oltre alle difficoltà di gestione dovute alla mancanza di competenze, comportano numerosi benefici tra cui la riduzione dei costi delle licenze, la resilenza, l'assenza di *storage*, la ridondanza e tutti i benefici di un'infrastruttura *open source*.

Centro Interservizi amministrativi

I "Centri Interservizi Amministrativi" (CIA), sono strutture deputate al coordinamento gestionale delle Sedi poste all'interno di una determinata area omogenea. Il CIA si pone ad un livello intermedio tra gli Uffici all'estero e la Farnesina, espletando una continua opera di raccordo che favorisce il superamento dei problemi e rafforza lo scambio informativo. In questo senso, essi rappresentano un nuovo punto di equilibrio nella dialettica fra autonomia e centralità. La struttura presiede al *procurement* per l'area di competenza, coordina la gestione amministrativo-contabile delle Sedi e il personale ad essa preposto ed affronta ogni tematica comune erogando attività di consulenza, supporto, analisi.

Il Centro interservizi è altresì chiamato a definire procedure uniformi e a rafforzare l'applicazione della normativa in materia di amministrazione digitale, contrasto alla corruzione, trasparenza. Il modello organizzativo è modulare, flessibile ed adattabile alle diverse realtà politiche e geografiche. Il primo Centro interservizi è stato istituito nel gennaio 2014 a Bruxelles ed è dedicato alle dieci Sedi presenti in Belgio, Olanda e Lussemburgo:

- tre Ambasciate (Bruxelles, L'Aia e Lussemburgo);
- due Rappresentanze permanenti, presso l'Unione europea e la NATO, entrambe a Bruxelles;
- due Consolati generali (Amsterdam e Charleroi);
- tre Istituti di cultura (Amsterdam, Bruxelles e Lussemburgo).

Il Centro negozia convenzioni e contratti quadro per la prestazione di servizi e la fornitura di beni aventi caratteri comuni, operando alla stregua di una vera e propria centrale di committenza. A tal fine, esso trae preziose indicazioni dall'analisi e dal monitoraggio delle scritture contabili delle Sedi interessate, sviluppando soluzioni attagliate al caso concreto e alle dinamiche di mercato dell'area di competenza. Tra gli elementi più innovativi del

procurement adottato vi è quello della transnazionalità, ovvero dell'estensione del mercato di approvvigionamento a un perimetro esteso oltre i confini statali, che favorisce la concorrenza e l'affermarsi di forniture ottimali. Il CIA opera come una piccola Consip, con lo scopo di uniformare la gestione e le procedure di ogni settore Tale soluzione rappresenta un valore aggiunto in quanto può essere facilmente trasposta anche all'interno dell'organizzazione statale, regionale e locale.

La struttura del CIA si regge sul *Cloud*, in particolare su un *software* gestionale in grado di condividere in remoto le risorse e i dati virtualizzati delle sedi di tutto il modo.

Corte dei Conti

L'iniziativa, realizzata in collaborazione con il CNEL e stimolata dalle sollecitazioni dell'Agid, si basa su un modello ispirato dal *cloud* per la condivisione di infrastrutture. In futuro, è prevista una collaborazione con la Società in house del Ministero dell'Economia e delle Finanze – SOGEI e con l'Avvocatura dello Stato, tra le più importanti pubbliche amministrazioni. Con quest'ultima è evidente la somiglianza strutturale e di ambito istituzionale, e si prevede di creare dei comparti intermedi simili con l'obiettivo finale di poter utilizzare lo stesso modello.

Il *framework* di integrazione ha seguito dei passaggi strutturati: in primo luogo è stata eseguita l'analisi logica dell'impatto, seguita poi dall'inclusione fisica, fino al terzo *step* con l'implementazione degli applicativi. Le prime due fasi sono state realizzate con il CNEL, tuttavia attualmente il progetto non si è ancora concluso.

Gran parte delle infrastrutture di base sono implementate in modalità *multi tenant*, grazie al quale è possibile intervenire lasciando una buona autonomia operativa alle singole amministrazioni.

L'iniziativa della Corte dei Conti ha portato numerosi benefici, soprattutto di tipo economico. In particolare, il modello si basa su una logica di economia di scala secondo cui una quota delle spese sostenute dalla Corte dei Conti è compensata dalle amministrazioni che beneficiano delle infrastrutture messe loro a disposizione. Pertanto, ogni quota versata dagli enti fruitori del servizio contribuisce ad abbassare i costi complessivi della gestione dell'IT da parte della Corte dei Conti.

Inoltre, i benefici si estendono anche alle amministrazioni ospitate dalla Corte dei Conti, come nel caso del CNEL il quale, prima dell'adesione all'iniziativa, non aveva previsto un sistema di *disaster recovery*, oggi implementato grazie all'inclusione nelle infrastrutture della Corte dei Conti, dotate di questo servizio.

Infine, come già si è avuto modo di evidenziare, le collaborazioni tra le P.A. favoriscono il riuso dei *software* e dei modelli adottati. Infatti, grazie ad una semplice estensione del contratto, la Corte dei Conti ha consentito al CNEL di poter utilizzare tutti gli applicativi gestionali e per la digitalizzazione dei fascicoli personali, saltando tutta la parte di analisi progettuale essendo già in uso ad un'altra pubblica amministrazione.

INAIL

L'INAIL è attualmente in attesa che si concludano le procedure per l'implementazione del Sistema Pubblico di Connettività per le P.A. in *Cloud*. Tuttavia, alcune iniziative di migrazione verso la "nuvola" sono già state intraprese da parte dell'Ente, con l'obiettivo di far fronte a future potenziali situazioni di scarsità delle risorse. Oltre 250 *server* sono stati implementati in *cloud*, utilizzando l'infrastruttura libera per il *back end*. Vi sono, poi, altri progetti più avanzati sulla *mobility* e progetti sperimentali tesi ad assicurare una maggiore efficienza per tutti i soggetti ed operatori coinvolti nei servizi offerti dall'organismo.

La fase di studio è durata circa otto mesi, durante i quali sono stati individuati gli obiettivi, definiti i *KPI* (*Key Performance Indicator*) di misura e quali utenti finali coinvolgere nel progetto. L'iniziativa ha coinvolto le direzioni centrali le quali, sulla base di conoscenze interne, hanno individuato alcuni operatori dipendenti Inail, operanti in territori complicati dal punto di vista geografico, che potessero testare l'uso dei nuovi applicativi *cloud*. Il progetto pilota prevedeva la riproduzione di un ambiente di lavoro organizzato attraverso la selezione di *device* implementati per lo *smartworking*.

I dipendenti avevano il compito di fornire costanti *feedback* sulle prestazioni e sull'uso delle nuove tecnologie introdotte che, in caso di riscontri positivi, potranno essere estese all'intero organigramma della pubblica amministrazione Inail.

Ministero degli affari esteri e della cooperazione internazionale

Nel 2012 è stata avviata un'iniziativa chiamata «M@E *Cloud*», volta alla realizzazione di una piattaforma aperta e multicanale in *private cloud*, per lo sviluppo e l'erogazione di applicazioni informatiche e nuovi servizi consolari per i cittadini italiani all'estero, i cittadini stranieri e le imprese, e di supporto alle attività di *back-office* dell'organizzazione interna. Tra i servizi disponibili in *cloud* vi sono ad esempio «Viaggiare sicuri», le borse di studio e le prenotazioni presso i consolati *on-line*, i concorsi e le informazioni per le imprese che intendono investire in un determinato Paese. L'iniziativa ha l'obiettivo di aumentare l'efficacia dei servizi offerti ai cittadini e alle imprese, riducendo i costi di gestione e aumentando la velocità e l'efficienza nello scambio di dati e informazioni. Il tutto è realizzato per garantire maggiore sicurezza, anche in termini di *disaster recovery*.

Sulla sicurezza il Ministero ha avviato un progetto pilota chiamato «LIMES – Linea informatica di Migrazione, Emergenza e Sicurezza» con lo scopo di rafforzare le misure di sicurezza informatica delle sedi diplomatico-consolari situate in aree ad alta conflittualità in modo che sia assicurata la continuità operativa, sia nella consultazione delle banche dati contenenti le informazioni sui cittadini italiani all'estero sia nell'erogazione dei servizi consolari, durante i periodi critici. L'iniziativa ha comportato la realizzazione di una infrastruttura informatica in *cloud*, attraverso la virtualizzazione e la configurazione di oltre 200 *server*. L'infrastruttura è in grado di condividere le banche dati e le informazioni con tutte le pubbliche amministrazioni coinvolte nell'ambito della politica estera, quali uffici consolari e rappresentanze all'estero.

Con l'implementazione di questa nuova infrastruttura *cloud* il MAE ha registrato un notevole risparmio economico, derivante dall'abbassamento dei consumi energetici, rispetto a quelli sostenuti in precedenza per alimentare l'intero apparato degli Uffici ministeriali e la Rete all'estero, con conseguente riduzione dell'impatto ambientale delle attività ICT ministeriali.

Inoltre, da non sottovalutare, l'iniziativa ha consentito anche un accrescimento delle competenze del personale dipendente e del valore complessivo delle capacità lavorative, favorendone così l'intercambio dei ruoli nella direzione IT.

Ministero delle Infrastrutture e dei Trasporti

Inizialmente il parco infrastrutturale del Ministero delle Infrastrutture e dei Trasporti era delocalizzato e distribuito sul territorio. Grazie alle tecnologie *cloud* è stato razionalizzato e consolidato, arrivando ad essere costituito da soli due *datacenter* in *cloud* privato, un unico *datacenter* logico unificato in cui risiedono tutte le applicazioni.

L'evoluzione del sistema prevede, nei prossimi anni, il collegamento con il *cloud* di Microsoft, un *data center* ibrido, per poter sfruttare la piattaforma One Drive, mettendo a disposizione degli utenti 1 TB di spazio in *cloud*. In questo modo sarà possibile accedere al sistema da qualunque postazione per lo scambio di documenti e la consultazione degli archivi.

Inoltre, è prevista la fornitura di servizi nel *cloud* pubblico per ciò che riguarda l'archiviazione delle *e-mail* sul *cloud* di Microsoft.

Ministero della Giustizia

Il Ministero della Giustizia, insieme alle iniziative di informatizzazione delle attività processuali, sta portando avanti un progetto di consolidamento *data center*, con progressi soprattutto sul settore penale dove, al posto di una piccola sala *server* residente presso ogni procura (140 in totale), vi sono oggi 26 sale distrettuali a copertura dell'intera rete nazionale. Nell'ambito della giustizia civile invece, attualmente vi sono 7 *data center* che potrebbero, a breve, diventare 3 per tutto il territorio nazionale. Il consolidamento delle infrastrutture, fortemente voluto anche dall'Agid, rappresenta un obiettivo ambizioso per il Ministero, incentivato anche dalla necessità di diminuire i costi.

Al contrario rispetto ad altre amministrazioni pubbliche, il Ministero della Giustizia non ha puntato verso un'evoluzione in *cloud*, tanto che non ha nemmeno aderito alla gara SPC della Consip per la gestione della posta elettronica e delle Pec.

In termini di private *cloud* sono presenti piattaforme di contabilizzazione e replica, mentre per quanto riguarda il *cloud* pubblico, questo è stato più volte proposto senza riscontri positivi dovuti, oltre alla mancanza di dinamicità nei requisiti di calcolo, anche all'impossibilità di esternare i dati per questioni legate alla *privacy*.

Regione Toscana

Il progetto "Tuscany Internet eXchange (TIX) 2.0", evoluzione del TIX 1.0 nato nel 2002,è un progetto sperimentale della Regione Toscana volto alla creazione di un centro servizi e di un centro tecnico di supporto per gli oltre 400 soggetti pubblici della Rete Telematica Regionale Toscana. Prevede inoltre la realizzazione di un punto di interscambio tra le reti degli ISP e le reti della P.A., di fatto anticipando di fatto gli effetti del Sistema Pubblico di Connettività.

Il progetto, con la trasformazione del *data center* in chiave *cloud*, rappresenta per la Regione un'opportunità di razionalizzazione della spesa. L'infrastruttura condivisa, infatti,consente alle singole amministrazioni di non acquistare le macchine e quindi di contenere i costi grazie a fattori di scala, fornendo addirittura livelli di servizio più elevati rispetto a quelli che potrebbero realizzare i singoli CED locali.

Per le amministrazioni fruitrici è stato predisposto un listino di servizi che va a coprire le componenti Iaas (*Infrastructure as a Service*) e PaaS (*Platform as a Service*) con le logiche di scalabilità e uso a domanda, tipiche del *cloud*. In prospettiva è prevista anche la fornitura di servizi SaaS (*Softwareas a Service*). I servizi IaaS offrono capacità computazionale, di memorizzazione e di rete, sulla quale l'utente può installare ed eseguire il *software* necessario, dal sistema operativo alle applicazioni. Attraverso i servizi PaaS il TIX fornisce e gestisce lo strato di *software* che si colloca sopra il sistema operativo (*application server* e *Dbms* per esempio) e supporta configurazioni sia *open source* sia *software* commerciale.

Infine, sono disponibili anche servizi di *housing*, *backup* aggiuntivo (oltre a quello base incluso nei servizi IaaS e Paas), servizi professionali, soluzioni per assicurare la continuità operativa.

1.2 La "Sanità Elettronica"

La digitalizzazione della Pubblica amministrazione passa non solo attraverso i processi di *e-Government* ed *e-School* fin qui esaminati, ma investe anche il settore sanitario. Il fenomeno è meglio conosciuto come "sanità elettronica" o "*e-health*" e indica il processo di migrazione dei servizi sanitari

verso una gestione, prevalentemente o interamente, informatica. Nell'ambito di questo processo evolutivo di ammodernamento della sanità pubblica e privata sono state intraprese numerose iniziative e introdotti vari strumenti finalizzati al miglioramento dell'efficienza dei servizi sanitari mediante un ulteriore sviluppo delle reti e una gestione sempre più ampia di atti, documenti e procedure, attraverso modalità informatiche e telematiche. È in questa direzione che devono inquadrarsi i progetti che hanno introdotto il Fascicolo e il Dossier Sanitario Elettronico, i Referti *on-line* e la Cartella Clinica Elettronica.

Il Fascicolo sanitario elettronico (FSE) è definito dall'art. 12 del d.l. 18 ottobre 2012, n. 179[15], come"*l'insieme dei dati e dei documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito*". Il FSE rappresenta quindi l'aggregazione dei dati e delle informazioni di natura sanitaria generati da ogni evento clinico riguardante un paziente ed è alimentato dai soggetti che operano nell'ambito del Servizio sanitario nazionale e dei servizi Socio-sanitari regionali. Il FSE è stato istituito con l'obiettivo di garantire, da una parte, la necessaria prevenzione, diagnosi, cura e riabilitazione in ambito medico e, dall'altra, di agevolare lo studio e la ricerca scientifica in ambito medico, biomedico e epidemiologico. Infine, la sua istituzione risponde anche all'esigenza di assicurare la programmazione sanitaria, verificare la qualità delle cure e valutare l'assistenza sanitaria.

Alla luce delle caratteristiche del FSE, appare evidente come il *cloud computing* rappresenti una soluzione tecnologica adottabile per la gestione e la condivisione dei dati e dei documenti da riversare nel Fascicolo[16]. At-

[15] Il decreto, noto anche come "D.L. Sviluppo *Bis*", è stato convertito con modificazioni dalla L. 17 dicembre 2012, n. 221

[16] In proposito si segnala l'art. 2 del d.p.c.m. 29 settembre 2015, n. 178, recante "Regolamento in materia di fascicolo sanitario elettronico", il quale ha previsto i contenuti del FSE sono rappresentati da un nucleo minimo di dati e documenti e da documenti integrativi. Per quanto riguarda il nucleo minimo questo è costituito da: "*a) dati identificativi e amministrativi dell'assistito di cui all'articolo 21; b) referti, inclusi quelli consegnati ai sensi del decreto del Presidente del Consiglio dei ministri 8 agosto 2013, pubblicato nella Gazzetta Ufficiale n. 243 del 16 ottobre 2013; c) verbali pronto soccorso; d) lettere di dimissione; e) profilo sanitario sintetico, di cui all'articolo 3; f) dossier farmaceutico; g) consenso o diniego alla donazione degli organi e tessuti*". I documenti integrativi, invece, sono elencati al comma 3 e possono

tualmente, però, nonostante il recente intervento normativo del d.p.c.m. 29 settembre 2015, n. 178, non si riscontrano interventi da parte del legislatore in questa direzione. Tuttavia, un riferimento al *cloud computing*, seppure in termini generali, è contenuto nel CAD in cui si prevede il *cloud* tra le soluzioni adottabili dalle Pubbliche Amministrazioni per acquisire i sistemi informatici nel rispetto dei principi di economicità ed efficienza, tutela degli investimenti, riuso e neutralità tecnologica[17].

Il Dossier sanitario elettronico è stato definito dall'Autorità Garante per la Protezione dei dati personali come l'insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l'interessato, messi in condivisione logica dai professionisti sanitari che lo assistono, al fine di documentarne la storia clinica e di offrirgli un migliore processo di cura. Tale strumento è costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti. Com'è agevole notare, il dossier rappresenta una evoluzione dello strumento del FSE, adottato da diverse strutture sanitarie per migliorare i processi di cura dei propri assistiti.

La Cartella clinica elettronica, introdotta dall'art. 47-bis del d.l. 9 febbraio 2012, n. 5 (convertito con modificazioni dalla L. 4 aprile 2012, n. 35) nell'ambito delle misure di semplificazione della sanità digitale, rappresenta l'atto pubblico in formato elettronico contenente la storia clinica di un paziente in riferimento ad un singolo ricovero o processo di cura ed è relativa ad una medesima struttura sanitaria. Quest'ultimo elemento la distingue dal FSE che, invece, è costituito da informazioni e dati appartenenti a più strutture.

Infine, il Referto *online* rappresenta, più semplicemente, la relazione scritta del singolo medico sullo stato clinico del paziente dopo un esame clinico o strumentale, rilasciata con modalità informatica.

L'evoluzione digitale della sanità pubblica consente la gestione e l'archiviazione dell'ingente mole documentale prodotta dagli organismi sa-

---

essere riversati a discrezione delle singole regioni, in base al livello di maturazione del processo di digitalizzazione.

[17] Cfr. Art. 68, co. 1, lett. d), d.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale), come modificato dal D.L. 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221, ove, per la prima volta, il legislatore italiano inserisce un chiaro riferimento al "*cloud computing*".

nitari nell'ambito dei processi di cura dei pazienti e agevola la gestione amministrativa dell'intero sistema sanitario. In tal senso, il fenomeno dell'*e-health* permette, da una parte, il risparmio in termini sia economici sia di risorse e, dall'altra, permette la realizzazione di nuove modalità di offerta dei servizi, come accade per il FSE e per la cartella clinica elettronica.

Oltre ai benefici già indicati, non bisogna trascurare l'importanza di ulteriori effetti della digitalizzazione: la continua disponibilità di tutte le informazioni sanitarie e la loro accessibilità in remoto da qualunque postazione abilitata; la completezza informativa, grazie alla standardizzazione dei formati utilizzati dalle strutture sanitarie ed alla condivisione dei dati a livello generale; infine, l'automazione di tutti i processi e degli adempimenti dei cittadini verso la P.A. e viceversa, con notevole risparmio di costi e di tempo sia per gli utenti che per l'amministrazione pubblica.

Alla luce delle sue caratteristiche, nell'ambito del processo di digitalizzazione della sanità pubblica, il *cloud computing* rappresenta una valida soluzione tecnologica per migliorare e potenziare il cammino verso una completa gestione informatizzata della sanità. In questo senso, *e-health* e *cloud computing* sono concetti sempre più interconnessi tra loro.

1.3 I più significativi contributi istituzionali dedicati al *cloud computing* in ambito sanitario.

Nell'ambito del presente lavoro, il principale settore d'interesse connesso al *cloud computing* è certamente quello sanitario.

Le già citate "*raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*" pubblicate da DigitPA il 10 luglio 2012 e il parere 5/2012[18] del Gruppo di lavoro "*ex* Art. 29 per la protezione dei dati dell'Unione Europea"[19] affrontano i più peculiari aspetti della

[18] Su tale parere si tornerà, per altri aspetti, nella parte quarta del presente lavoro.

[19]Il Gruppo "Article 29 *data protection working party*" è stato istituito con la Direttiva 95/46/CE, art. 29 (dal quale, appunto, prende il nome). Si tratta di un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.
Tra i compiti più significativi del Gruppo (disciplinati dall'art.30 della Direttiva) vi sono:

tecnologia *cloud* al comparto sanitario. In particolare le Raccomandazioni di DigitPA si preoccupano, in primo luogo, dell'esatta individuazione della tipologia di dati da migrare sul *cloud*: "*comuni, sensibili (e tra questi i dati sanitari), giudiziari*". In via generale si evidenzia che il passaggio al *cloud* va calibrato sulla specie del trattamento eseguito e delle criticità connesse al trattamento dei dati coinvolti, anche al fine di individuare le responsabilità

- l'esame esaminare delle questioni attinenti all'applicazione delle norme nazionali di attuazione della direttiva;
- la formulazione di pareri sul livello di tutela nella Comunità e nei paesi terzi;
- attività consultiva nei confronti della Commissione in merito ad ogni progetto di modifica della Direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà;
- la formulazione di pareri sui codici di condotta elaborati a livello comunitario;
- la formulazione di propria iniziativa di raccomandazioni su qualsiasi questione riguardi la protezione dei dati personali nella Comunità;
- la definizione di criteri di adeguatezza per i paesi terzi.

Il Gruppo, altresì, interviene, informando la Commissione, qualora vi siano delle divergenze tra le legislazioni degli stati membri che possano pregiudicare l'equivalenza della tutela persone. Il gruppo ha la possibilità, inoltre, di formulare di propria iniziativa delle raccomandazioni su qualsiasi questione riguardante la tutela dei dati personali nella Comunità. I pareri e le raccomandazioni del gruppo vengono trasmessi di regola alla Commissione, la quale è tenuta, a sua volta, ad informare il Gruppo del seguito dato ai suoi pareri e raccomandazioni.

Il gruppo si riunisce in plenaria in media ogni due mesi, approva all'inizio dell'anno un programma di lavoro di massima in cui vengono indicate le priorità operative. Il gruppo ha costituito negli anni vari sottogruppi di lavoro incaricati di seguire le singole questioni e tematiche.

Per quanto concerne gli aspetti di organizzazione e funzionamento, il Gruppo è dotato di un suo regolamento interno ed un documento generale sulla strategia. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Le decisioni sono adottate a maggioranza semplice dei rappresentanti delle autorità di controllo.

Redige una relazione annuale, che trasmette alla Commissione, al Parlamento ed al Consiglio e che pubblica. In essa sono illustrati l'operato e gli sviluppi in materia, tenendo conto sia dell'attività svolta nell'ambito del gruppo sia degli aspetti più rilevanti dell'attività condotta dalle autorità garanti nazionali.

I provvedimenti adottati dal Gruppo sono indicati da un numero di riferimento (ad es. WP3), sono ordinati cronologicamente, disponibili dal 1997 ad oggi ed elencati al presente link: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm, unitamente ad altre informazioni utili ed ai riferimenti alle autorità nazionali di controllo. I documenti sono disponibili anche sul sito *web* dell'Autorità Garante per la protezione dei dati personali (http://www.garanteprivacy.it), con una scheda esplicativa di accompagnamento.

dei principali soggetti coinvolti: il *buyer* (così è definito l'ente che acquista il servizio in *cloud*) e il *provider* (ossia, il fornitore del servizio).

In tutto ciò, una particolare attenzione, in quanto ritenuto *"campo di applicazione particolarmente fertile del* cloud"[20] con un "*grado di complessità e di implicazioni particolarmente elevato*", è rivolta alla gestione del fascicolo sanitario elettronico. "*Qui si può solo rilevare da un lato che il* cloud *si presenta come una tecnologia particolarmente vantaggiosa nella gestione del fascicolo sanitario elettronico, sia sotto il profilo del contenimento della spesa, sia sotto quello dell'efficienza, dell'interoperabilità e della implementazione di stringenti misure di sicurezza, e che dall'altro lato il trattamento deve attestarsi ad un livello particolarmente rigoroso di rispetto delle regole fondamentali in materia di tutela dei dati personali: stretta aderenza alla finalità, pertinenza e non eccedenza, durata limitata del trattamento (compatibilmente con le finalità), rispetto della dignità dell'interessato e dei suoi familiari, corretta e completa informativa, pieno controllo da parte dell'interessato sui propri dati. Tra i vari aspetti tecnologico-giuridici si segnala come il rigoroso controllo degli accessi logici, l'accurata gestione delle identità e dei relativi privilegi al trattamento dei dati, nonché la conservazione dell'integrità dei medesimi risultano condizioni necessarie per la migrazione – a norma di legge – verso il* cloud *di tali servizi*"[21].

Anche nel parere 5/2012 del Gruppo di lavoro "*ex* Art. 29 per la protezione dei dati dell'Unione Europea" è presente una parte espressamente dedicata alle precauzioni da adottare nel *cloud* del settore pubblico. Si esprime chiaramente la necessità di particolari cautele che l'ente pubblico deve valutare tutte le volte che il *cloud* comporta "*la comunicazione, il trattamento e la conservazione di dati fuori dal territorio nazionale*"[22]in quanto vi è il concreto pericolo di "*esporre a rischi inaccettabili la sicurezza e la* privacy *dei cittadini, nonché la sicurezza e l'economia nazionale, in particolare se sono coinvolte banche dati sensibili (ad es. dati del censimento) e servizi (ad*

[20] DigitPA, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, 2012, p. 35-36.
[21] *ibidem*.
[22] Gruppo di Lavoro Art. 29 per La Protezione Dei Dati, Parere 05/2012 sul *cloud computing*, 2012, p. 26.

es. servizi sanitari)[23]". Il parere procedeva con un auspicio, oggi diventato realtà[24] affinché i governi nazionali e le istituzioni dell'Unione europea approfondissero ulteriormente il concetto di *cloud computing* europeo conregole coerenti e armonizzate.

Nella medesima direzione si mosse anche l'*Authority* italiana con due distinti documenti[25] contenenti entrambi l'obbiettivo di offrire un primo insieme di indicazioni utili per l'adozione consapevole e responsabile di servizi in modalità *cloud computing*. Le avvertenze contenute nei documenti del Garante privacy italiano sono ovviamente focalizzate a favorire il corretto trattamento dei dati personali, volendo rappresentare un primo quadro di cautele nell'adozione di servizi in *cloud.* Persiste, anche nelle dichiarazioni del Garante italiano, un elemento di continuità con quanto detto anche in precedenza, ossia la consapevolezza che l'utilizzo dei servizi di *cloud computing* "*prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale, e in considerazione di tutte le sue implicazioni in relazione al trattamento dei dati personali*". Su queste basi, il Garante dichiara espressamente l'intento di continuare a seguire l'evoluzione del fenomeno, anche partecipando con altri decisori istituzionali a specifici tavoli

[23] Su tali aspetti si tornerà più diffusamente nella parte quarta del presente lavoro, ove saranno illustrati gli aspetti più significativi del rapporto elaborato dall'ENISA dal titolo "sicurezza e resilienza in *cloud* governativi. Di particolare interesse in questa sede è la parte del documento in cui si esprime che: "*in termini di architettura, per applicazioni sensibili le soluzioni* cloud *private e di comunità sembrano essere quelle che attualmente rispondono meglio alle esigenze delle pubbliche amministrazioni perché offrono il massimo livello di* governance, *controllo e visibilità, anche se nel pianificare un sistema* cloud *privato o di comunità si dovrebbe prendere in particolare considerazione la scala dell'infrastruttura*".

[24] Il 14 aprile 2016 è stato approvato il Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati). Il regolamento sarà pubblicato a breve nella Gazzetta ufficiale dell'Unione Europea, ed entrerà in vigore 20 giorni dopo. Le nuove disposizioni saranno direttamente applicabili in tutti gli Stati membri due anni dopo tale data.

[25] "Il *cloud computing*: indicazioni per l'utilizzo consapevole dei servizi", pubblicato (in data 16 novembre 2011 e consultabile all'indirizzo *web* http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1819933) e il "*cloud computing*: proteggere i dati per non cadere dalle nuvole" (pubblicato in data 24 maggio 2012 e consultabile all'indirizzo *web* http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1894503)

di lavoro aperti in materia, in particolare con DigitPA (oggi Agenzia per l'Italia Digitale o semplicemente AgID) per quanto attiene all'adozione di modelli orientati alle *cloud* in ambito pubblico.

Poco tempo dopo, infatti, anche l'AgID avviava una consultazione pubblica in ordine alla bozza delle linee guida intitolate "caratterizzazione dei sistemi *cloud* per la Pubblica Amministrazione"[26]. Il documento elaborato dall'AgID mostra un particolare interesse per il *cloud computing* nell'ambito del Sistema Pubblico di Connettività (SPC)[27] rilevando alcune problematiche di interoperabilità costituite dalla "sicurezza e dalla privacy" e con l'intento di fornire dei ragionevoli indirizzi.

La stessa Agenzia compie espresso riferimento al *cloud computing* nella "*Linee Guida per il Disaster Recovery (DR) delle Pubbliche Amministrazioni*", che nella versione aggiornata (2013) sono il frutto di un lavoro congiunto fra AgID, Pubbliche Amministrazioni e rappresentanze dei fornitori di servizi di *cloud computing*. In esse si tiene conto della disciplina dettata in tema di sicurezza informatica e tutela dei dati personali, nonché dei provvedimenti del Garante privacy[28]. Nel documento il *cloud computing* e inquadrato quale interessante alternativa ai modelli tradizionali di *disaster recovery* e il principale punto di forza dei servizi di *DR* basati sul *cloud* riguarda il vantaggioso rapporto tra costi e prestazioni: a fronte di tempi di ripristino

[26] Il documento è consultabile al seguente indirizzo *web*http://www.agid.gov.it/sites/default /files/linee_guida/sistemi_cloud_pa.pdf

[27]Il Capo VIII, del D. Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale (CAD) – è dedicato al Sistema Pubblico di Connettività (SPC) e rete internazionale della pubblica amministrazione, che trova la sua definizione all'art. 73, comma 2°: "*Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione*".

[28] Sugli aspetti relativi alla protezione dei dati personali, si veda il Parere del Garante privacy sullo schema di "Linee-guida per il *Disaster Recovery* delle Pubbliche Amministrazioni", emanate ai sensi dell'articolo 50-bis, comma 3, lett. b), del Codice dell'amministrazione digitale del 4 luglio 2013, consultabile al seguente indirizzo *web* http://www.garanteprivacy.it/web/ guest/ home/docweb/-/docweb-display/docweb/2563133

simili a quelli delle soluzioni basate su risorse dedicate, i costi sono di poco superiori all'ipotesi di risorse condivise[29].

Nello scenario fin qui considerato, non si può certamente trascurare l'ambito normativo europeo, da una parte, con il cosiddetto "pacchetto Telecom"[30] e, dall'altra, con la recente approvazione del nuovo Regolamento generale sulla protezione dei dati[31]. In particolare, quest'ultimo, standardizzando la disciplina in tutto il territorio europeo, rende più affidabili e sicuri i servizi di *cloud computing* anche attraverso l'estensione dell'obbligo di notifica delle violazioni di sicurezza che riguardino dati personali a tutti i titolari del trattamento dei dati, come ad esempio le ASL: gli utenti interessati saranno, in tal modo, tempestivamente informati in caso di perdita o furto dei loro dati.

1.3.1 Il *vademecum* su *Cloud* e sanità

Tra i più significativi interventi afferenti al rapporto tra i servizi di *cloud computing* e il settore sanitario non può essere trascurato il documento che nel 2013 è stato redatto e pubblicato da Federsanità-ANCI[32] e Istituto Italia-

[29] Le linee guida in esame illustrano i molteplici vantaggi del *cloud computing* con espresso riferimento, tra gli altri, alla natura flessibile della fruizione di risorse in modalità *on demand* (ossia, pagate in base all'uso), che comporta un investimento iniziale molto basso; ai tempi molto ridotti per l'avvio della soluzione di *DR* sono ridotti ; alla notevole facilità ed economicità delle attività di test. Nel documento, però, non mancano aspetti critici connessi alla natura particolare dei servizi *cloud* che ogni Pubblica Amministrazione deve tenere in considerazione, per le ovvie ricadute in tema di protezione dei dati personali. Dei principali vantaggi e criticità del *cloud computing* si tratterà più diffusamente nella parte quarta del presente lavoro.

[30] Il riferimento è alle Direttive 2002/58/CE (cosiddetta "e-privacy"), Direttiva 2009/136/CE (che modifica la precedente con l'inserimento della cookie law) e Direttiva 2009/140/CE. Le ultime due recepite in Italia con i decreti legislativi 28 maggio 2012, n.ri 69 e 70.

[31] Regolamento del Parlamento europeo e del Consiglio n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

[32] Dal sito istituzionale, in http://www.federsanita.it/html/chi_siamo/it/presentazione.asp "*Federsanità-ANCI (Associazione Nazionale Comuni Italiani) è il soggetto istituzionale che organizza Aziende Sanitarie Locali e Ospedaliere e Conferenze dei Sindaci e che agisce come strumento sul piano della rappresentanza per i Comuni per assicurare i percorsi di integrazione sociosanitaria e socioassistenziale. Nata nell'ottobre 1995 come una Federazione di Aziende USL, di Aziende ospedaliere e di Comuni con l'intento di contribuire fattivamente al processo di aziendalizzazione e di integrazione dei servizi innescato a partire fin dall'inizio*

no Privacy[33]. Si tratta di un documento che, a differenza di quelli (di natura istituzionale sopraccitati) non ha un contenuto precettivo ma certamente interessante per l'ampia portata rappresentativa delle due associazioni redattrici.

Elemento costante, anche nel *vademecum*, è il fattore risparmio, quale principale motivo propulsore della scelta di servizi in *cloud*. Ancora una volta si constata che alla base della scelta vi è l'abbattimento dei costi fissi per l'acquisto di strumenti informatici (*hardware* e *software*), nonché per la manutenzione e aggiornamento degli stessi. Con la migrazione verso la "nuvola" la spesa (certamente ridotta) è esclusivamente concentrata sull'ottenimento del servizio (e sui relativi livelli) parametrato ai concreti bi-

---

degli anni '90, nell'ottobre 2006, durante il primo Congresso Nazionale Federsanità-ANCI, si trasforma in confederazione di federazioni regionali. La Confederazione è attualmente composta da 17 federazioni regionali ed annovera tra i propri associati 166 Aziende Sanitarie e le relative Conferenze dei Sindaci".

[33]Dal sito istituzionale, in http://www.istitutoitalianoprivacy.it/it/chi-siamo/ "*L'Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP) è un centro di ricerca e di* advocacy *finanziato anche da soggetti privati (persone fisiche, associazioni, studi legali e aziende anche multinazionali) dedicato alle tematiche della protezione e della valorizzazione dei dati personali, dell'informazione e dell'identità nella società globale dell'ICT. L'Istituto coinvolge e mette in relazione molti tra i migliori specialisti italiani del diritto della privacy ma anche significativi rappresentanti degli ambiti pubblici e privati che con i dati personali, spesso sensibili, lavorano quotidianamente. Operando come* think tank*, l'IIP è punto di riferimento per gli esperti italiani del "nuovo diritto" e per i diversi player dei mercati ad elevato contenuto tecnologico. L'Istituto utilizza come principali strumenti di azione il sito internet, dove vengono pubblicati i contributi dei propri Soci* Fellow *e di altri ricercatori, e una newsletter informativa quindicinale con le principali notizie e analisi sulle evoluzioni delle problematiche privacy in Italia e nel mondo. Si organizzano con frequenza trimestrale convegni aperti al pubblico e* workshop *seminariali a porte chiuse, dove possibile in partnership con realtà universitarie nazionali ed europee, per favorire la formazione dei professionisti e insieme per sensibilizzare i non addetti ai lavori, siano essi operatori di mercato o istituzioni pubbliche: tali incontri vengono sempre trasmessi anche in* web-tv *e* web-radio*, attraverso il portale dell'Istituto, e resi disponibili per il* download *o per la visualizzazione in modalità* streaming*. Tra le ulteriori attività, annoveriamo una intensa produzione di articoli e altri generi di interventi per diversi* media-partner *(quotidiani, riviste, tv, radio,* web*), la pubblicazione della Rivista scientifica Diritto, economia, tecnologie della Privacy, alla quale si uniranno in futuro la diretta pubblicazione di libri sulla privacy da parte dell'Istituto e l'assegnazione su base semestrale di borse di studio in materia di diritto dell'ICT, secondo i criteri stabiliti di volta in volta dal Comitato Scientifico e in base alle disponibilità economiche deliberate per ogni esercizio*".

sogni di struttura (quindi flessibile). In tal modo, i fruitori del servizio (amministrazioni pubbliche e private) realizzano delle concrete economie, che potranno essere reimpiegate in differenti direzioni.

Il fattore risparmio, però, seppure basilare, non è l'unico ad essere preso in considerazione *excursus* contenuto nel documento, si pone, infatti, in risalto l'ampia utilità dei sistemi *cloud* che devono essere pensati e utilizzati "*non solo per l'archiviazione o* storage *di dati sanitari, ma anche per la fruizione in* cloud *di potenti applicativi sanitari (ad esempio il FSE) o per lo sviluppo dei medesimi su apposite piattaforme* software *in* cloud"[34].

Rinviando alla lettura integrale del *vademecum*, di seguito si riepilogano le cinque parti principali in cui è suddiviso:

- illustrazione delle caratteristiche essenziali nella scelta del *cloud computing* in ambito sanitario;
- analisi delle misure di sicurezza che i soggetti pubblici devono osservare quando vanno in *cloud*;
- esame di alcune specifiche aeree della sanità elettronica (referti *on-line*, cartella clinica elettronica e fascicolo sanitario elettronico)
- sintesi per singoli documenti sanitari d'uso comune, non condivisi in *dossier* o fascicolo sanitario elettronico, che possono essere realizzati con *software* di lavoro "classici" per l'ufficio basati sulla tecnologia-*cloud computing* (prenotazioni, registri, riepiloghi/*report*, immagini, documenti clinici, comunicazioni verso l'utenza ecc.);
- *checklist* come strumento pratico per potenziali fornitori che offrono servizi *cloud* agli operatori sanitari pubblici e, per questi ultimi, come guida utile per la fase di trattativa contrattuale con i suddetti fornitori.

2. La carta di Castelfranco

Un'importante tappa del *Cloud computing* applicato al comparto sanitario è rappresentata dalla Carta di Castelfranco, che sintetizzai lavori svoltisi durante il Convegno di Castelfranco Veneto, promosso da Forum PA e dall'Azienda Ulss 8 di Asolo, il 18 ottobre dell'anno 2011. Nell'occasione, per la prima volta in Italia, si sono riuniti esperti e studiosi che hanno di-

[34] p. 3.

scusso sui vari aspetti economici, tecnologici e giuridici riguardanti l'applicazione del *Cloud Computing* nel settore sanitario.

La Carta di Castelfranco rappresenta un documento unico nel suo genere e costituisce un punto di riferimento per tutti gli operatori del settore, *cloud provider*, soggetti privati, enti e pubbliche amministrazioni interessati all'adozione dei servizi in *cloud* per la sanità. Infatti, oltre ai notevoli vantaggi gestionali ed economici, il *cloud* presenta anche alcuni aspetti critici che è necessario affrontare per ridurre al minimo il rischio conseguente all'adozione di tali soluzioni.

Con lo sviluppo dell'*e-Health*, il *digital divide* che ancora colpisce molte strutture sanitarie e che varia da Paese a Paese e da settore a settore, è accompagnato da un nuovo fenomeno: il "*cloud computing divide*". Quest'ultimo consiste nella nascita di una netta divisione tra amministrazioni sanitarie all'avanguardia, in grado di offrire servizi avanzati ad un costo contenuto grazie al *cloud*, e strutture sanitarie meno sensibili alla nuova tecnologia costrette a spendere di più per offrire servizi non sempre all'altezza delle possibilità e delle richieste dell'utenza. In questo contesto, la Carta di Castelfranco, con i suoi vincoli e la sua visione in prospettiva, rappresenta un punto di riferimento per le amministrazioni sanitarie interessate ad evolvere verso il *cloud computing*.

Prima di affrontare nello specifico il contenuto della Carta di Castelfranco, è opportuno riprendere alcuni aspetti sul *cloud*, in parte già visti, che hanno ispirato la redazione delle dodici raccomandazioni in essa contenute.

In primo luogo, le potenzialità del *cloud computing* sono tali da consentire ad un'azienda sanitaria, che ha già intrapreso il percorso di informatizzazione, di potenziare le proprie infrastrutture e di migliorare i servizi in modo facile e veloce; allo stesso tempo, con l'adozione di soluzioni *cloud* anche un'amministrazione sanitaria meno solerte può rapidamente colmare il *gap* con le altre strutture più progredite dal punto di vista informatico.

Le aziende sanitarie che adottano soluzioni *cloud*, infatti, non devono affrontare più tutti quei problemi, tra cui la formazione di competenze specialistiche interne nel settore ICT o l'acquisto e il ricambio periodico di hardware, che negli ultimi decenni hanno determinato forti rallentamenti nella gestione e trasmissione dei dati.

Altre semplificazioni derivano dalla possibilità di acquistare servizi su richiesta (dalla radiologia, ai servizi di pronto soccorso, alla cardiologia, e così via), senza dover passare attraverso le lunghe e complesse fasi di analisi, progettazione ed esecuzione, perché l'acquisto è limitato al solo servizio.

Con il *cloud computing*, quindi, si può realizzare il massimo risultato anche per un sistema sanitario attualmente poco all'avanguardia, con uno sforzo notevolmente ridotto.

Per queste ragioni è fondamentale elaborare un piano strategico, una *roadmap* come viene definita anche nelle raccomandazioni della Carta di Castelfranco, da parte di tutte le amministrazioni sanitarie che intendono passare al *cloud computing*.

In primo luogo, è necessario determinare quelle che sono le caratteristiche dell'attuale assetto tecnologico aziendale e le prospettive che il mercato offre per il miglioramento dei servizi, in considerazione delle varie modalità di offerta dei servizi *cloud* (*IaaS*, *PaaS*, *SaaS*). Questa fase è seguita dalla determinazione dei costi per gli interventi programmati, in correlazione con le risorse economiche disponibili.

L'ultima fase, infine, è costituita dalla definizione dei livelli minimi di servizio (*Service Level Agreement*) con il *provider*, il quale deve essere in grado di garantire tutti i servizi che l'amministrazione sanitaria ha il compito di erogare.

L'analisi qui descritta può essere rappresentata graficamente con un percorso a piramide a struttura progressiva, ove ogni fase della struttura costituisce una solida base per l'avanzamento verso il livello superiore.

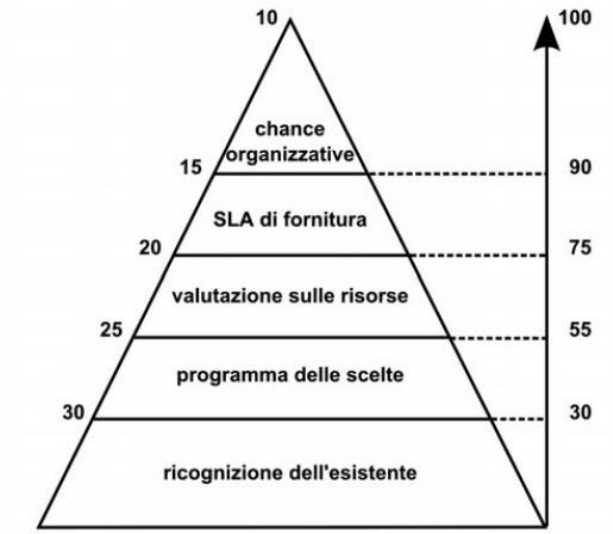

Figura 13: L'analisi piramidale per il passaggio al *cloud computing*[35]

2.1 Le raccomandazioni della Carta di Castelfranco

Le dodici raccomandazioni contenute nella Carta di Castelfranco possono essere suddivise in cinque macroaree, ognuna delle quali comprende delle raccomandazioni per uno specifico obiettivo o ambito.

Le prime tre raccomandazioni riguardano aspetti legati alle condizioni e alle attività preliminari all'adozione del *cloud computing*:

1. "*Operare con una rete a banda larga ridondata, per la connessione tra strutture ospedaliere, medici, cittadini e* provider[36].

2. *Accertare preliminarmente l'utilizzabilità del "*private cloud*", prima di decidere di avvalersi di un "*public cloud*"*[37].

[35] Fonte: *Cloud Computing in sanità Un nuovo paradigma di sviluppo*, Gruppo24Ore, 2012, p. 62.

[36] Ogni sistema basato su tecnologie interconnesse non può, infatti, prescindere dall'adozione di un adeguato mezzo di trasmissione delle informazioni.

[37] Le differenze tra il *public cloud* e il *private cloud* sono già state ampiamente descritte nella prima parte del presente lavoro, in "Modelli di implementazione e tipologie di *cloud*". Tuttavia, con questa raccomandazione si intende invitare le strutture sanitarie a privilegiare soluzioni *private* per le caratteristiche di personalizzazione, controllo e governo dei dati e affidabilità, meno garantite in un sistema *public*. Per le definizioni del *cloud* si rimanda alla parte prima del presente lavoro "*Modelli di servizio: dall'infrastruttura alle applicazioni*".

3. *Predisporre una* roadmap *per portare al* cloud computing *i sistemi ospedalieri disponibili, secondo condizioni sostenibili di tipo economico, gestionale e di sicurezza*[38]".

Nei punti successivi sono fornite alcune indicazioni in tema di garanzia per il fruitore di servizi in *cloud*:

4. "*Accertare la conservazione dei dati clinici in* data center *situati in un Paese U.E., con garanzia di applicazione delle norme e della giurisdizione italiane, se diverse da quelle europee*[39].

5. *Richiedere ai provider garanzie di:*

- *Interoperabilità tra sistemi ospedalieri intra*-cloud, *inter*-cloud *e sistemi* cloud *con no*-cloud*;*
- *Portabilità dei dati nei casi di passaggio ad altro fornitore*[40].

6. *Richiedere ai* provider *garanzie di continuità operativa permanente dei sistemi in* cloud computing[41]".

Ulteriori raccomandazioni riguardano le attività di controllo da parte del fruitore di servizi *cloud*:

7. "*Specificare la* policy *di gestione del fornitore per l'attività di salvataggio/* backup *dei dati clinici* on the cloud[42].

8. *Monitorare l'esclusione di ingerenze esterne nei dati clinici cloud, consentendo sempre l'accesso ai sistemi da parte delle autorità preposte*[43]".

I seguenti due punti si riferiscono, in particolare, alla figura del *cloud provider*:

---

[38] L'importanza di una pianificazione è direttamente proporzionale alla complessità della struttura presso la quale si intende adottare il sistema *cloud*.

[39] La raccomandazione intende focalizzare l'attenzione sulle problematiche della residenza dei dati immessi nel *cloud*, trattate nella parte quarta del presente lavoro.

[40] Interoperabilità tra sistemi e portabilità dei dati sono aspetti fortemente collegati, l'assenza dell'uno non consente il realizzarsi dell'altro. La tematica è stata già approfondita nella parte seconda.

[41] La continuità operativa, com'è già stato sottolineato più volte, è un aspetto cruciale per le amministrazioni sanitarie che devono garantire in modo continuativo i loro servizi. Cfr. nota n. 1 della parte quarta.

[42] Il *backup* dei dati è una delle misure minime richieste dal D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali".

[43] Il tema è stato oggetto di approfondimento nella parte quarta, al paragrafo dedicato al controllo e governo sui dati del *cloud*.

9. "*Formalizzare la responsabilità del provider nelle ipotesi di smarrimento, perdita e sottrazione dei dati clinici, sospensione della continuità operativa, crisi di interoperabilità*[44].

10. *Verificare la confidenza dei* provider *rispetto ai processi clinici e all'organizzazione ospedaliera*[45]".

Infine, le ultime due raccomandazioni riguardano l'organizzazione della struttura dell'azienda sanitaria:

11. "*Disporre l'evoluzione della struttura ICT ospedaliera verso competenze* service management[46].

12. *Istituire un "*Privacy and risk manager *ospedaliero" per la protezione, gestione, sicurezza dei dati clinici*[47]".

La Carta di Castelfranco costituisce, quindi, una valida fonte di regole e prassi che tutti i consumatori di *cloud computing* nella sanità digitale dovrebbero seguire affinché siano mitigati e, talvolta, evitati i rischi e le criticità insite nel *cloud*.

2.2 Il *management* del *cloud*

La raccomandazione n. 11 della Carta di Castelfranco pone una questione molto rilevante per le aziende del SSN. L'attuale immobilismo delle strutture sanitarie e ospedaliere in tema di informatizzazione dei processi e dei servizi è dovuto alla presenza di elevati costi di gestione rispetto ai benefici ricavabili. Tuttavia, con l'adozione di soluzioni basate sui modelli del *cloud computing* questa tendenza può essere invertita e l'*ICT*, da elemento di

[44] La responsabilità in caso di eventi dannosi è un punto nodale del rapporto tra le strutture sanitarie e il *cloud provider*. In proposito, si veda quanto illustrato nella parte quinta del presente lavoro.

[45] L'affidabilità del fornitore dei servizi deve essere valutata anche alla luce della sua competenza nel settore sanitario che, per le sue peculiarità, differisce dagli altri settori dove normalmente vengono offerti servizi in *cloud*. In questo senso, un altro aspetto rilevante è dato dagli anni di esperienza e dal *curriculum* aziendale del *cloud provider*.

[46] Con il *cloud*, le strutture sanitarie acquisiscono servizi per erogare altri servizi. Per queste ragioni, è necessario investire sulla gestione dei servizi e sul miglioramento degli stessi.

[47] La figura del "*privacy and risk manager*" sarebbe il punto di riferimento all'interno della struttura sanitaria per la gestione delle criticità legate alle tecnologie *cloud*, fin qui esaminate.

ostacolo, potrebbe divenire lo strumento per una evoluzione in positivo dell'intero settore sanitario.

Con il *cloud*, i responsabili della gestione dei sistemi informativi aziendali[48] si trovano a gestire infrastrutture meno rigide e più economiche; in questo modo, il patrimonio tecnologico dell'azienda, da costo fisso, può trasformarsi in fattore di evoluzione, sia in termini di qualità che economici. Il CIO avrà sempre più un ruolo di management dell'IT aziendale e non più un mero ruolo tecnico. La missione dei futuri responsabili dei sistemi informativi non sarà più limitata all'acquisizione di soluzioni IT, ma si estenderà anche sul piano del business finalizzato alle soluzioni aziendali.

Per queste ragioni le strutture sanitarie devono investire e sviluppare nuove competenze in grado di affrontare le nuove sfide poste dal *cloud computing*.

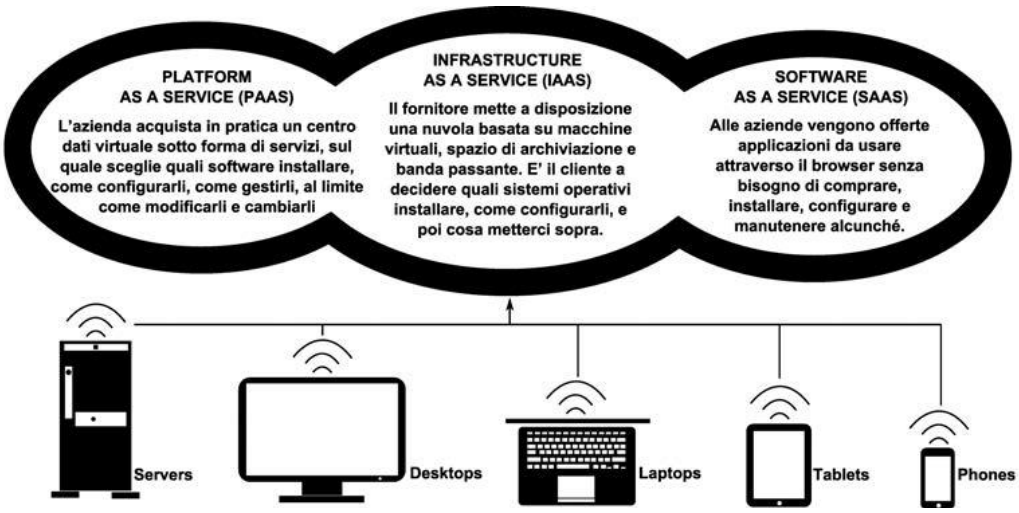

Figura 14: I modelli del *cloud computing*[49]

2.3 Il rapporto del *cloud provider* con il mondo sanitario

Nella decima raccomandazione si suggerisce di verificare la confidenza dei *provider* rispetto ai processi clinici e all'organizzazione ospedaliera. Il concetto di confidenza è molto più della semplice conoscenza e significa che il *cloud provider* deve essere ben consapevole di tutte le implicazioni relati-

[48] *Chief Information Officer* (CIO)

[49] Fonte: *Cloud Computing in sanità Un nuovo paradigma di sviluppo*, Gruppo24Ore, p. 65

ve alla gestione e all'organizzazione di una struttura sanitaria, compresa l'etica e la cultura di questi ambienti.

La confidenza deve essere valutata in relazione sia ai sistemi tecnologici, professionali, operativi, normativi ed economici sia in riferimento ai processi clinici e gestionali della cura dei pazienti. Infine, confidenza significa altresì conoscenza del linguaggio medico, dell'etica professionale e dell'azione sanitaria. Il mondo della tecnologia deve poter dialogare con quello della medicina e viceversa; solo così potranno essere adottate soluzioni tecnologiche in grado di rispondere efficacemente alle esigenze delle strutture sanitarie e, conseguentemente, dei pazienti. Da ciò, è evidente la necessità di investire per un percorso di specializzazione di nuove figure in grado di gestire l'implementazione e il successivo management del *cloud computing* per la sanità.

Un ulteriore fronte di interesse per i redattori della Carta di Castelfranco è la collocazione dei *data center* e la conservazione dei dati.

È indubbio che il *cloud computing* sia un fenomeno globale oramai inarrestabile, per la facilità di implementazione e per tutti i vantaggi che offre. Come accade ogni volta che si diffonde l'uso di una nuova tecnologia, è necessario valutare se le regole in vigore, in quanto applicabili, garantiscano una tutela sufficiente e non costituiscano, invece, un ostacolo alla sua diffusione, con conseguente limitazione dei vantaggi per l'intera società.

In generale, le regole applicabili a questo nuovo paradigma non sono pienamente adatte a favorirne la diffusione e l'utilizzo su larga scala. Ciò risulta confermato anche dalla raccomandazione che prevede la conservazione dei dati clinici in data center situati in un Paese U.E.. La scelta, che raccoglie le indicazioni provenienti dalle massime istituzioni comunitarie, essendo basata sull'attuale sistema di regole, non tiene conto della realtà del mercato. Infatti, molte aziende e fornitori di servizi in *cloud* conservano dati sanitari (provenienti dalle più svariate attività, dal telecontrollo dei cardiopatici, alle immagini cliniche ed alla posta elettronica del personale sanitario) fuori dal territorio europeo.

Alla luce di ciò, affinché il *cloud computing* possa diffondersi nel pieno rispetto delle garanzie e dei diritti dei cittadini di tutto il mondo, sarebbe auspicabile che siano emanate nuove regole pensate *ad hoc* per questo complesso fenomeno, che tengano conto delle sue caratteristiche tecniche, delle

sue criticità e delle esigenze dei consumatori del *cloud*. Secondo un'indagine EUROSTAT[50], infatti, tra i maggiori fattori di ostacolo che limitano l'uso del *cloud computing*, vi sono nell'ordine: il rischio di violazioni della sicurezza dei dati, l'incertezza sulla legge e sulla giurisdizione applicabile, l'incertezza sull'ubicazione dei dati, problemi di accesso ai dati e ai *software*, le difficoltà nell'accesso alle informazioni, le criticità nella cessazione del rapporto o nella migrazione verso un altro provider. La figura 15 riassume quanto detto finora.

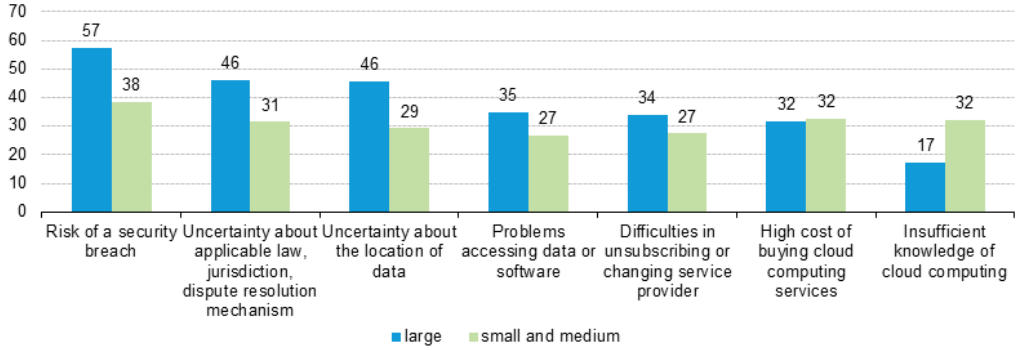

Figura 15: *Factors limiting enterprises from using* cloud computing *services*[51]

Le nuove regole, quindi, dovrebbero rappresentare un modo per accompagnare il *cloud* verso un utilizzo più consapevole, riducendo i rischi e senza limitarne le potenzialità.

2.4 L'impatto sul mondo del lavoro

Il risparmio economico derivante dall'adozione di modelli basati sul *cloud computing*, consentirà di destinare nuove risorse economiche per gli investimenti e per l'innovazione.

Così come il *cloud computing* rappresenta un cambiamento radicale per molte imprese e amministrazioni pubbliche, il fenomeno rappresenta anche un motivo di cambiamento per il mondo del lavoro, non solo legato all'ICT,

[50] Lo studio "*Cloud computing - statistics on the use by enterprises*" è consultabile all'indirizzo web:http://ec.europa.eu/eurostat/statistics_explained/index.php/Cloud_computing_statistics_on_the_use_by_enterprises

[51] Fonte: Eurostat

ma anche ad altri settori. In parte questo cambiamento è stato già illustrato quando si è parlato del nuovo ruolo del CIO[52].

Il passaggio al *cloud* ha portato ad un aumento della domanda di lavoro per professionisti e *manager* specializzati in *business development*, nonché alla nascita di nuove professionalità tra le quali: *cloud capacity planners*, *cloud service manager*, *cloud architects*. Altre nuove figure professionali non necessariamente accompagnate nel titolo dalla parola "*cloud*", sono fortemente legate ad esso[53]. Inoltre, secondo una ricerca condotta da Microsoft si è stimato che, nel periodo dal 2012 al 2015, nel mondo si sarebbero generati quasi 14 milioni di posti di lavoro grazie al *cloud computing*[54].

Tuttavia, questo forte impatto nel mondo del lavoro, deve essere rapportato e valutato anche in relazione alla diffusione del *cloud computing* all'interno del settore lavorativo. In particolare, per il settore sanitario[55], l'uso del *cloud* è più basso, secondo solo al settore dell'industria delle risorse. Per queste ragioni, insieme agli altri profili di criticità già ampiamente dibattuti, gli effetti di crescita occupazionale nel settore sanitario è più debole rispetto ad altri comparti.

[52] Cfr. par. 5.2, Parte Terza.

[53] Secondo una stima della Commissione Europea, nel 2015 il settore ICT in Europa ha registrato oltre 900.000 opportunità di lavoro, molte delle quali nel settore del *cloud computing*. Per un approfondimento, v. "*net-cloud future*", European Commission's DG CONNECT - Directorate-General for Communications Networks, Content and Technology (2013)

[54] Secondo lo studio, intitolato "*Cloud computing's role in job creation*", Microsoft-Idc (2011), si stimava una crescita sensibile dei posti di lavoro in tutti i Paesi del mondo. In particolare: 125% in Italia, 137% in Francia, 108% nel Regno Unito, 135% in Germania, 139% in Spagna. In altri Paesi meno sviluppati, la crescita è ancora più elevata, fino a toccare una stima pari a circa il 400% nei Paesi sudamericani.

[55] Come mostrato nella figura n. 16

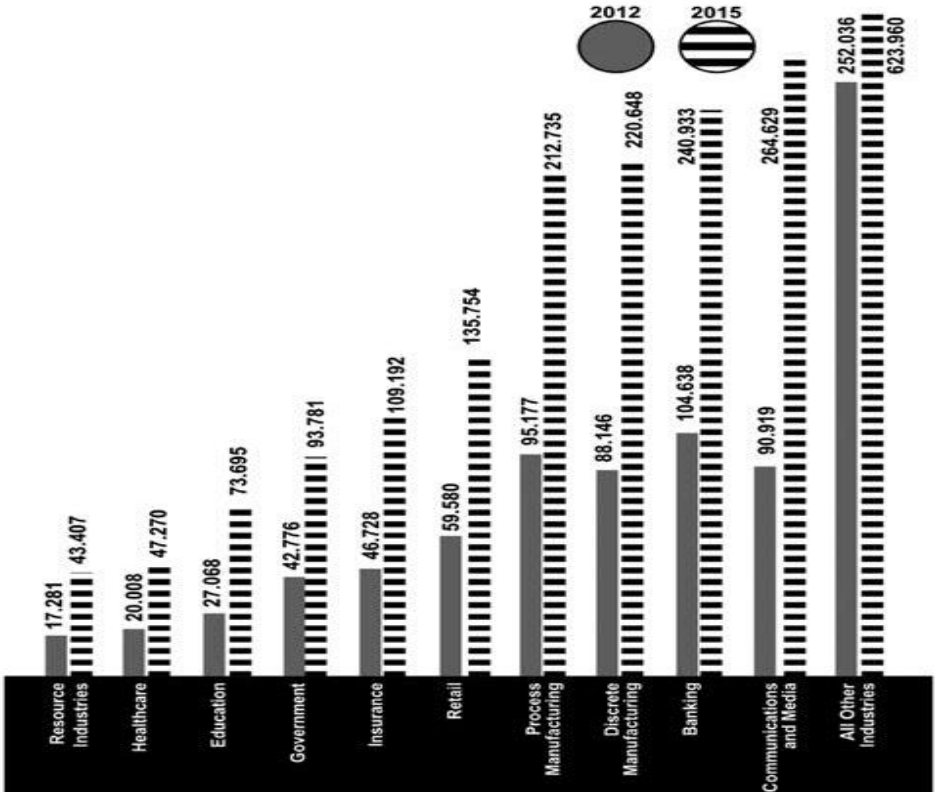

Figura 16: La crescita occupazionale grazie al *cloud computing*[56]

3. Indagine pilota sui servizi sanitari in Piemonte del Centro Nexa su Internet e Società del Politecnico di Torino[57]

Nel periodo compreso tra febbraio e giugno 2012, il Centro Nexa su Internet e Società del Politecnico di Torino[58] ha condotto un'indagine diretta alla rilevazione dello stato dell'arte sulla distribuzione e l'impiego delle risorse informatiche da parte delle pubbliche amministrazioni e alle opportu-

[56] Fonte: Microsoft-Idc (2011)

[57] L'indagine ha interessato le seguenti amministrazioni sanitarie: ASL n. 3 di Collegno e Pinerolo, ASL di Asti e Azienda Ospedialiera O.IR.M. Sant'Anna di Torino.

[58] Il Centro Nexa su Internet e Società del Politecnico di Torino (Dipartimento di Automatica e Informatica), fondato nel novembre 2006, è un centro di ricerca indipendente che studia le componenti della forza di Internet e i suoi effetti sulla società. Comprendere Internet, identificarne limiti e potenzialità, è indispensabile per assicurare sviluppo economico, tecnico-scientifico, culturale e politico per gli anni a venire.

nità che potrebbero conseguire dall'adozione di soluzioni incentrate su modelli di *cloud computing*. L'analisi è stata condotta su un'area territoriale (quella piemontese) considerata rappresentativa[59] del contesto nazionale con particolare riguardo ai servizi maggiormente nevralgici per il cittadino e più diffusi sul territorio oggetto di indagine. La suddetta indagine ha preso in esame i tre seguenti settori: – amministrazioni locali (comuni, unioni di comuni, comunità montane); – servizi scolastici (scuole dell'infanzia, primarie, secondarie di I grado, secondarie di II grado); – servizi sanitari (Aziende Sanitarie Locali, Aziende Ospedaliere). Proprio l'ultimo dei tra settori esaminati è di particolare interesse per la tematica affrontata nel presente lavoro, seppure limitata all'ambito della Regione Piemonte, che, per la numerosità della popolazione, per la distribuzione sul territorio dei servizi "in *cloud*", per la varietà territoriale (socio-economica e tecnologica) essa rappresenti un esempio di particolare significatività (non in termini statistici) all'interno del panorama nazionale.

Diversamente dagli altri settori della pubblica amministrazione, quello sanitario è indubbiamente tra i più complessi dal punto di vista strutturale ed organizzativo. Nel settore sanitario, infatti, l'uso delle infrastrutture informatiche varia costantemente, alternando continuamente periodi di maggiore e minore impiego delle risorse[60]. Inoltre, data la criticità dei servizi erogati dalle strutture sanitarie (medicina d'urgenza, ricoveri, pronto soccorso), sempre operativi 24/7, è necessario che sia garantita la massima disponibilità delle risorse informatiche dedicate[61].

Nell'ambito dei servizi sanitari piemontesi sono già state adottate diverse soluzioni basate sul paradigma *client/server* per la gestione dei flussi informativi e dei dati, sul modello del *cloud*. In particolare, gran parte delle informazioni a livello regionale (dal pagamento delle quote ai medici di base,

[59] La scelta di limitare l'indagine all'ambito della Regione Piemonte è costituita dal fatto che, in ragione della numerosità della popolazione, della distribuzione sul territorio dei suddetti servizi, della varietà territoriale, socio-economica e tecnologica, essa rappresenta, in termini quantitativi un esempio di particolare significatività (in termini qualitativi e non statistici) all'interno del quadro nazionale.

[60] In altri settori come, ad esempio, le amministrazioni scolastiche l'uso delle risorse aumenta nei periodi in cui si concentrano particolari adempimenti burocratici.

[61] Particolari criticità si rilevano nei servizi connessi ai flussi di comunicazione interna alla struttura sanitaria, che richiedono l'impiego di sistemi avanzati per la gestione dei filtri e delle priorità nonché un elevato livello di affidabilità.

alle prestazioni specialistiche, di pronto soccorso, diagnostiche, di *day hospital*, alle impegnative, nonché le informazioni finanziarie relative a bilanci e rendicontazione) sono gestite con le suddette modalità. Allo stesso modo sono gestite le informazioni verso altri enti centrali (certificazioni di malattia, INAIL, e così via). In tale contesto, spesso accade che le strutture sanitarie affidino i servizi informatici a soggetti esterni, mentre tutti i servizi di memorizzazione, di *backup* e di gestione documentale, dal punto di vista informatico, sono strutturati su modelli simili al *cloud*.

Gli applicativi e i *software* necessari per implementare tali sistemi sono acquistati direttamente da fornitori privati, i quali elaborano spesso soluzioni personalizzate sulla base delle esigenze delle singole amministrazioni sanitarie. Contrariamente ad altri settori e in ragione della competenza delle Regioni in materia, nella sanità non vi è un'unica amministrazione centrale impegnata nell'elaborazione e nel rilascio di *software* agli enti minori.

Tra i *software* in uso nelle amministrazioni sanitarie è necessario distinguere, da una parte, gli applicativi gestionali e, dall'altra, i *software* che forniscono strumenti per l'erogazione di servizi verso il paziente (es. la cartella clinica elettronica). Nella regione Piemonte si è riscontrato che i *software* gestionali sono, per lo più, forniti da grosse aziende, mentre il mercato legato agli applicativi strumentali si presenta più variegato e frammentato, in ragione della maggiore esigenza di personalizzazione. Infatti, ciascuna ASL o ente sanitario necessita di differenti livelli e tipologie di servizio in relazione sia al territorio in cui operano sia alle scelte effettuate dal personale dirigente (dirigenti, primari, e così via). L'autonomia riservata a questi ultimi, rappresenta un forte ostacolo al raggiungimento di un'uniformità nelle scelte e nelle soluzioni *cloud* adottate nella sanità.

L'indagine svolta ha, quindi, posto in evidenza come la frammentarietà e l'esigenza di personalizzazione ha indotto le grandi imprese del mercato *IT* a non fornire più applicativi per la sanità, tranne che per gli applicativi gestionali. Inoltre, diverse soluzioni *software* per la fornitura di servizi sono offerti da altri fornitori di servizi collegati[62].

[62] Tale è il caso di un software per la gestione della cartella clinica fornito da una casa farmaceutica, oppure l'applicativo per il laboratorio di analisi offerto dagli stessi produttori di sistemi di analisi.

Per tali ragioni, il settore sanitario è caratterizzato dalla presenza di notevoli ostacoli all'adozione di un sistema uniforme per tutte le strutture che, invece, rappresenterebbe la soluzione ideale per garantire un'efficiente cooperazione tra le varie sedi e strutture del complesso sistema della sanità pubblica.

3.1 Contesto di riferimento e stato dell'arte

L'indagine condotta dal Centro Nexa è stata riferita a tre strutture sanitarie (due Aziende Sanitarie Locali e un'Azienda Ospedaliera) le quali presentano notevoli differenze sia nel numero di utenti/pazienti, sia nel numero di sedi e di lavoratori dipendenti.

La prima struttura è l'ASL di Asti che, con i suoi 2200 dipendenti, fornisce i propri servizi a circa 180mila cittadini; stessi numeri, seppur con un bacino inferiore di sedi fisiche, si registrano anche per la seconda struttura, l'O.I.R.M. Sant'Anna; il terzo Ente, l'ASL di Pinerolo, accoglie circa 500mila pazienti e 4500 dipendenti.

Ciascuna delle tre strutture ha sviluppato un volume dati di oltre 10 *terabyte* (tutte hanno la connessione con rete in fibra e reti LAN), destinati ad aumentare anno dopo anno, anche in ragione delle diverse tipologie documentali archiviate che, talvolta, incidono notevolmente sul volume di *storage* complessivamente utilizzato (ad esempio, le immagini della diagnostica, come ecografie o radiografie, sono contenute all'interno di file molto grandi in termini di spazio di memoria occupato).

Sotto il profilo organizzativo, le risorse umane impiegate per ciascuna delle realtà in esame variano tra i 6 e i 12 dipendenti con competenze informatiche, anche avanzate (più del 60% delle strutture è dotato di un ufficio legale). In tal senso, va specificato che le Amministrazioni operano grazie all'impiego prevalente di postazioni *desktop* e, in misura ridotta, di postazioni *mobile* (*laptop* e *smartphone*).

Per quanto attiene al parco applicativi, oltre alle varie *suites* da ufficio e i programmi forniti in modalità SaaS, è frequente l'uso di *software* per la si-

curezza dei sistemi e per la gestione dei portali *web*[63] (solo nell'AO Sant'Anna è in uso un servizio di *e-mail* dedicato). Si consideri, altresì, che in ognuna delle strutture sono adottati differenti modalità per il controllo degli accessi alle risorse informatiche e, in conformità alla disciplina prevista in materia di trattamento con strumenti elettronici di dati sensibili, sono adottate soluzioni per la trasmissione dei dati in modalità crittografata.

Per le dotazioni *hardware*: presso la ASL di Pinerolo sono in funzione 30 *cluster* di *server*, 11 presso l'AO Sant'Anna e un *cluster* con quattro nodi virtualizzati presso l'ASL di Asti. Inoltre, ciascuna è dotata di un *data center*, ridondato per ragioni di continuità di servizio, e un sistema di *backup* delle librerie presso il rispettivo fornitore dei servizi informatici.

La tipologia di servizi individuata è di quadruplice natura: amministrativi, gestionali, diagnostici e quelli connessi agli adempimenti di legge verso altri Enti Pubblici. In particolare, alcuni servizi gestionali e amministrativi, come ad esempio la gestione stipendi e la pianificazione dell'utilizzo delle risorse (ERP), sono forniti grazie ad applicativi rilasciati dal Consorzio per i Sistemi Informativi (CSI Piemonte) sul modello SaaS[64]. Le attività di diagnostica avvengono mediante l'uso di applicativi che consentono la raccolta, la catalogazione, l'archiviazione e la conservazione di tutte le informazioni necessarie (è doveroso precisare che i *software* utilizzati per queste finalità variano a seconda della struttura e del singolo reparto o specialità medica). I flussi informativi relativi alle prestazioni e ai ricoveri sono trasmessi alla Regione tramite interfaccia fornita dalla CSI Piemonte. Le informazioni relative alle attività di Pronto Soccorso e alla diagnostica d'urgenza effettuata nelle autoambulanze sono, invece, condivise grazie all'infrastruttura denominata RUPAR Piemonte (Rete Unitaria della Pubblica Amministrazione in Piemonte)[65] .

Per quanto attiene, infine, all'ultima categoria di servizi citati, questi avvengono sempre mediante interfaccia fornita dalla CSI Piemonte e si sostanziano nell'obbligo di trasmissione di informazioni ad atri Enti, quali, ad e-

[63] Nelle strutture oggetto della presente indagine si registra l'uso di *software* non proprietario (*server* Linux e Open Office) per un totale di due casi su tre.

[64] Vedi l'applicativo ERP TrakCare: http://www.intersystems.com/trakcare/index.html.

[65] Vedi il Progetto TEMPORE (Teleconsulto Medico Piemonte Ospedali in Rete).

sempio, le informazioni relative alla gestione dell'organico dipendente verso l'INAIL.

L'indagine condotta dal centro Nexa, non poteva ignorare uno dei principali fattori che spingono la Pubblica amministrazione a migrare verso soluzioni in *cloud*, ossia l'aspetto economico. In tal senso è risultato che i costi delle infrastrutture *IT* sono coperti grazie ad una spesa pari a circa l'1% del bilancio complessivo degli Enti esaminati:

- per l'A.O. Sant'Anna, circa 300mila euro/annui per gli applicativi (comprese le relative licenze), 500mila euro per il personale informatico, 100mila euro per la connettività e 200mila euro per l'acquisto, gestione e manutenzione *hardware*;
- per l'ASL di Asti, la fornitura dei servizi informatici è garantita da una convenzione, in scadenza nel luglio 2018, con un raggruppamento temporaneo di imprese per complessivi 3 milioni di euro, di cui 1 milione per la gestione *hardware*, circa 1 milione di euro per la gestione del personale informatico (20 unità on site e reperibilità 24/7), 800mila euro per la gestione dei *software* (comprese le licenze), 650mila euro per la manutenzione degli applicativi, 300mila euro per l'*hardware* e, infine, 110mila euro per la connettività.

Se, come risulta dall'indagine quivi brevemente riassunta, alcuni modelli adottati dalle strutture sanitarie piemontesi per i servizi di *storage* e per la gestione documentale, sono di tipo *cloud computing*[66], ve ne sono alcuni non ancora gestiti in tale modalità, tra cui quello della posta elettronica, che rappresenta una parte importante dell'attività delle strutture sanitarie. L'esigenza di elevate prestazioni, di affidabilità e di continuità operativa richiesti dai servizi di posta elettronica, ben potrebbero, infatti, essere soddisfatti grazie all'adozione di modelli basati sul *cloud computing*, anche alla luce dei pluricitati vantaggi di scalabilità e contenimento dei costi, tanto cari alla Pubblica Amministrazione.

[66] È questo il caso dell'ASL di Asti che ha affidato alla società Telecom, capofila del RTI, la gestione dei servizi IT attraverso un'infrastruttura *cloud*.

PARTE QUARTA - VANTAGGI E CRITICITÀ DEL *CLOUD COMPUTING* IN AMBITO SANITARIO

1. I principali vantaggi

Al pari di ogni settore della P.A., anche per la sanità pubblica, organismo dotato di una struttura complessa ed articolata, sono numerosi i benefici che possono derivare dall'adozione delle tecnologie *cloud*.

Da una parte, si distinguono vantaggi di tipo organizzativo, che consistono nella sistematizzazione delle infrastrutture, nella riorganizzazione dei flussi informativi e conseguentemente, nel miglioramento della fruibilità dei dati all'interno del sistema. Dall'altra, quale diretta conseguenza dei primi, vi sono indubbi vantaggi economici e razionalizzazione dei costi, dovuti alla presenza di servizi più moderni, più efficienti e più funzionali.

Non è un caso che, anche il DigitPA in passato si sia espresso in modo favorevole nei confronti del *cloud*, definendolo come uno dei mezzi più economici per assicurare ad una gran parte dei servizi di *e-government* caratteristiche di efficacia, efficienza, trasparenza, partecipazione, condivisione, cooperazione, interoperabilità e sicurezza.

Le infrastrutture *cloud* consentono di abbandonare le vecchie logiche legate all'uso di grandi e potenti macchinari, come accadeva con i *mainframe* o i *data center* locali, che necessitavano di competenze e risorse umane in grado di gestirli e quindi di rilevanti spese.

Per sua natura, la tecnologia di *cloud computing* è molto più semplice e facilmente integrabile con l'infrastruttura esistente: le applicazioni sono generalmente accessibili tramite un semplice *web browser* e ciò le rende quasi completamente indipendenti dai sistemi già in uso presso l'Ente; a ciò si aggiunga il vantaggio pratico della semplicità di configurazione, di avvio e di gestione. Inoltre con il *cloud*, a differenza di quanto accadeva in passato, l'Ente che intende aggiornare la propria infrastruttura IT non deve più fare i conti con la compatibilità dei propri *server*, dei *client* e dei sistemi operativi utilizzati. Con l'uso del *web browser*, che sostituisce il tradizionale rapporto *client-server*, le macchine già in uso all'Ente sono destinate ad una vita più

lunga in quanto non è più necessaria una potenza sempre maggiore di elaborazione. Infatti, le infrastrutture condivise su cui vengono ospitate le applicazioni *cloud* sono progettate per garantire un'erogazione costante di potenza elaborativa all'aumentare delle istanze applicative e del numero di utenti attivi.

Si supera totalmente il concetto di aggiornamento del *software* in uso e di tutto ciò che ne consegue in termini organizzativi, di sicurezza e di costi, in quanto le applicazioni in *cloud* vengono aggiornate direttamente dal fornitore del servizio sull'infrastruttura condivisa (nella quale risiedono), dopo accurati collaudi effettuati "*off-line*".

Inoltre, le infrastrutture di *cloud computing* assicurano la cosiddetta *Business Continuity* (o continuità operativa)[1], ossia prevedono modalità di ripristino di emergenza più rapide ed efficaci, nonché tempi di inattività dovuti a malfunzionamenti e/o manutenzione straordinariamente bassi. Infine, la gestione dei dati in *cloud* consente alle amministrazioni sanitarie di mettere in condivisione le proprie informazioni con altre strutture pubbliche, rendendo più efficiente il sistema attraverso un accesso rapido alle stesse.

Tutto ciò conduce verso un notevole risparmio economico, per lo meno sui costi di gestione ed amministrazione dell'infrastruttura IT.

Questo perché, in primo luogo, le spese di mantenimento e di aggiornamento dei *software* restano a carico del *cloud provider*; in secondo luogo perché la flessibilità dei servizi offerti in soluzioni *cloud*, consente all'Amministrazione di investire solo in caso di necessità e, quindi, le restanti risorse economiche possono essere utilizzate per altri investimenti ritenuti più urgenti.

[1] L'art. 50-bis del CAD, prevede che le amministrazioni predispongano dei piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. Il principio è quello della continuità operativa e obbliga le amministrazioni ad effettuare una valutazione preliminare sulle garanzie offerte dagli stessi *cloud provider*. Infatti, tra gli adempimenti della pubblica amministrazione, è prevista la definizione di un piano di continuità operativa, sottoposto a verifica biennale, 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. Pertanto, nel caso in cui i servizi offerti in cloud non assicurino la sicurezza dei dati, affinché sia comunque rispettato l'obbligo previsto dall'art. 50-bis del CAD, sarebbe opportuno che le pubbliche amministrazioni conservino *in-house* una copia di tutti i dati immessi nella rete *cloud*.

Il risparmio nei costi di acquisto dell'*hardware* e del *software* è riscontrabile anche nel valore economico dei canoni d'uso, che risultano essere notevolmente inferiori al costo[2] totale delle licenze d'uso delle applicazioni *client-server* analoghe. Le applicazioni in *cloud*, infatti, non necessitano di un'infrastruttura centrale dedicata, i cui costi per l'alimentazione elettrica di funzionamento e di condizionamento superano di gran lunga quelli di acquisto. Inoltre, i grandi *cloud provider*, a differenza degli operatori locali, possono collocare le proprie sedi in luoghi dove il costo dell'energia è più favorevole, così da poter ridurre ulteriormente il canone del servizio.

Infine, vi è un ulteriore aspetto vantaggioso (meno immediato di quelli appena illustrati) costituito dalla riduzione della spesa per il lavoro umano da dedicare alla gestione dell'infrastruttura. Con il *cloud computing* non è necessario, ad esempio, un amministratore di sistema per ogni singolo *server*, bensì sarà sufficiente un unico professionista che segue contemporaneamente più *cloud server*, anche di clienti diversi e/o eterogenei (pubblici e privati).

1.1 Le più significative tappe nazionali e internazionali *pro-cloud*

Tanto a livello nazionale, che a livello internazionale, soprattutto negli ultimi anni, vi sono stati interventi istituzionali in tema di *cloud computing*, ciò è sintomatico della sensibilità che i governi hanno maturato in materia.

La prima concreta presa di posizione italiana a favore del *cloud* è rappresentata dalle più volte citate "*raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*" (del 28 giugno 2012) pubblicate da DigitPA il 10 luglio 2012. Contemporaneamente, il Gruppo di lavoro "*ex* Art. 29 per la protezione dei dati dell'Unione Europea" adottava il parere n. 5 nel cui allegato vengono fornite le definizioni delle varie tipologie di *cloud*[3]. Entrambi i documenti sopraccitati mostrano un chiaro tenta-

[2] Tale costo va calcolato sommando il prezzo delle singole licenze d'uso, degli aggiornamenti periodici, dei contratti di manutenzione *software*.

[3] Per le definizioni del *cloud* si rimanda alla parte prima del presente lavoro "*Modelli di servizio: dall'infrastruttura alle applicazioni*".

tivo di standardizzazione, delle molteplici facce del *cloud computing*, totalmente proiettato verso il rispetto dei basilari principi di trasparenza, sicurezza e certezza giuridica da assicurare ad ogni fruitore di tali servizi.

Nel mese di settembre dello stesso anno la Commissione Europea pubblicava la Comunicazione intitolata "sfruttare il potenziale del *cloud computing* in Europa"[4] diretta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni.

Si trattava di una precisa presa di posizione a favore del *cloud computing*, che ne illustra le caratteristiche e i vantaggi in tutto lo scenario europeo. Una chiara strategia della Commissione "*volta a consentire e facilitare una più rapida adozione del* cloud computing *in tutti i settori dell'economia, adozione che può ridurre i costi* ICT *e, in combinazione con le nuove pratiche di* business *digitale, può aumentare la produttività, la crescita e l'occupazione*"[5].

Il contenuto dell'atto è riassumibile in tre azioni fondamentali:

1. districare il groviglio di norme[6];
2. rendere sicure ed eque le clausole contrattuali[7];
3. promuovere una *leadership* comune tra il settore pubblico e quello privato (industriale) per stabilire quali siano le esigenze e far sì che l'industria europea delle tecnologie dell'informazione sia in grado di soddisfarle[8].

---

[4] Consultabile al seguente *link*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[5] Cfr. M. MANCARELLA, *E-health e diritti, l'apporto dell'informatica giuridica*, 2012, p. 208.

[6] Il riordino normativo può garantire agli utenti la migrazione da una "nuvola" all'altra in maniera semplice e indolore. In tal senso, la Commissione si impegna a promuovere concrete azioni di standardizzazione e di certificazione (dei servizi offerti dai *cloud providers*) a livello europeo.

[7] La Commissione invita verso l'individuazione e la diffusione di buone pratiche riguardanti le clausole contrattuali tipo che permetteranno di accelerare l'adozione dei servizi di *cloud* e di aumentare per ciò stesso la fiducia dei potenziali consumatori futuri. Sostiene, inoltre, che l'intervento in maniera opportuna sulle clausole contrattuali può giovare anche al settore cruciale della protezione dei dati personal.

[8] Anche il settore privato godrebbe dei vantaggi di servizi di qualità più elevata, di una maggiore concorrenza, di una normazione rapida e di un'interoperabilità maggiore, senza contare le opportunità di mercato per le PMI, che potrebbero tenere testa più efficacemente alla

Nelle conclusioni la Commissione esortava gli Stati membri ad accogliere a piene mani il potenziale rappresentato dal *cloud computing* e li invitava a sviluppare una propria nuvola del settore pubblico in base ad approcci comuni in grado di migliorare le prestazioni e la fiducia e di ridurre i costi. Sosteneva, altresì, l'essenzialità della partecipazione attiva al partenariato europeo per il *cloud computing* e della divulgazione dei suoi risultati.

Sempre nell'anno 2012, il 26 ottobre, in occasione della 34ª Conferenza Internazionale su "*Data Protection ad Privacy*", svoltasi a Punta del Este-Canelones (Uruguay), fu adottata la Risoluzione sul *cloud computing*[9], nella quale furono inserite le seguenti raccomandazioni:

- "*Cloud computing should not lead to a lowering of privacy and data protection*
- *standards as compared with other forms of data processing;*
- *Data controllers carry out the necessary privacy impact and risk assessments (if necessary, by using trusted third parties) prior to embarking on CC projects;*
- *Cloud service providers ensure that they provide appropriate transparency, security, accountability and trust in CC solutions in particular regarding information on data breaches and contractual clauses that promote, where appropriate, data portability and data control by cloud users; cloud service providers, when they are acting as data controllers, make available to users, where appropriate, relevant information about potential privacy impacts and risks related to the use of their services.*
- *Further efforts be put into research, third party certification, standardisation, privacy by design technologies and other related schemes in order to achieve a desired level of trust in CC; to build privacy thoroughly and effectively into cloud computing adequate measures should be embedded into the architecture of IT systems and business processes at an early stage (privacy by design);*

---

concorrenza, specie a quella statunitense (si veda il par. 2.3 "Trasferimento di dati personali verso gli USA: dal Safe Harbor al Privacy Shield").

[9] Il documento è consultabile al seguente *link*: http://www.garante*privacy*.it/web/guest/home/docweb/-/docweb-display/docweb/2150634

- *Legislators assess the adequacy and interoperability of existing legal frameworks to facilitate cross-border transfer of data and consider additional necessary privacy safeguards in the era of CC, and*
- *Privacy and Data Protection Authorities continue to provide information to data controllers, cloud service providers and legislators on questions relating to privacy and data protection issues*".

Il documento si chiudeva con un concreto invito, per tutti gli *stakeholders* (operatori e clienti del *cloud computing*, nonché autorità di regolamentazione) per la cooperazione finalizzata alla garanzia di un elevato livello di protezione della *privacy* e dei dati.

2. Le principali criticità

Prima di affrontare nel merito gli aspetti critici della materia, è bene ripartire dalla definizione di *cloud computing*.

La computazione "nuvolare" rappresenta un concetto molto ampio, utilizzato spesso per definire genericamente la virtualizzazione o l'esternalizzazione dei servizi e delle attività. In assenza di una definizione normativa del *cloud*, è necessario rifarsi a due autorevoli definizioni di *cloud computing*, certamente utili in questa sede. La prima è la definizione ufficiale del *National Institute of Standards and Technology* (*NIST*) afferma che "*cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*"[10];

[10] "*Il* cloud computing *è un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore*", in P. MELL, T. GRANCE, *The NIST Definition of Cloud Computing: Recommendation of the National Institute of Standards and Technology*, NITS, US Department of Commerce, Gaithersburg (MD)2011.

La seconda definizione è quella elaborata dall'Autorità Garante per la protezione dei dati personali per la quale con l'espressione *cloud computing* si fa riferimento a un insieme di tecnologie e di modelli di servizio che "*favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via* web*; promuovono a seconda dei casi il trasferimento dell'elaborazione o della sola conservazione dei dati dai computer degli utenti ai sistemi del fornitore dei servizi*"[11].

Alla luce delle definizioni riportate e delle caratteristiche tecniche dei sistemi *cloud*, gli aspetti maggiormente critici di questi sistemi, di interesse in questa sede, riguardano tre aspetti principali: la circolazione dei dati sanitari, l'esternalizzazione e la delocalizzazione dei sistemi e dei servizi (con il rischio di perdita del controllo diretto ed esclusivo dei dati) e, infine, la conservazione dei dati in luoghi geografici spesso regolati da discipline differenti.

Come si può notare, le criticità rilevate sono tutte strettamente connesse al concetto di dato personale, così come inteso dalla normativa di cui al d. lgs. 196/2003 (definizione oggi confluita nel nuovo Regolamento Generale sulla Protezione dei Dati[12]). La disciplina dettata in materia di protezione dei dati personali assume un ruolo preminente in quanto la natura delle operazioni effettuate con le tecnologie *cloud* e la gestione dei flussi documentali, implica il compimento di una serie di operazioni che costituiscono, a tutti gli effetti, trattamento[13] di dati personali. Inoltre, con particolare riferimento al

---

[11] Garante per la protezione dei dati personali, "Cloud computing, *proteggere i dati per non cadere dalle nuvole*", la guida del Garante della *Privacy* per imprese e pubblica amministrazione, maggio 2012 http://www.garante*privacy*.it/web/guest/home/docweb/-/docweb-display/docweb/ 1894503.

[12] La definizione di "dato personale" contenuta nell'art. 4, n. 1) del Regolamento Privacy contiene tutti gli elementi già presenti nella omonima definizione del D.lgs. 196/03, con qualche ulteriore specificazione. Alla luce della più recente disciplina è, quindi, "dato personale": "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

[13] Anche la definizione di "trattamento", seppure sostanzialmente invariata, ha subito qualche formale modifica, così, l'art. 4, n. 2) del Regolamento lo definisce come: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a*

settore sanitario, le informazioni trattate sono di natura sensibile[14], con tutto ciò che ne consegue in termini di elevati livelli di sicurezza e particolari adempimenti a carico del titolare previsti dalla normativa.

Il primo aspetto critico del *cloud computing* è riferito alla circolazione dei dati. In merito a questo il Codice della *privacy* (D.lgs. 196/03) distingue, *in primis*, il trattamento dei dati sanitari compiuto da soggetti pubblici, da una parte, e quello effettuato da soggetti privati e da enti pubblici economici, dall'altra. Mentre i soggetti pubblici sono vincolati al principio di legalità, i soggetti privati e gli enti pubblici economici necessitano della manifestazione del consenso dell'interessato.

Il nuovo Regolamento Privacy, non conserva, almeno dal punto di vista strutturale, la distinzione sulla base della qualificazione pubblica o privata del titolare per stabilire la disciplina del trattamento dei dati sanitari (e degli altri dati sensibili e giudiziari). La disciplina (art. 9) è basata sul divieto, da considerare come principio di carattere generale, di trattamento dei dati personali che rivelino "*origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*". Tale divieto è, però, mitigato da una serie di deroghe[15] elencate dalla medesima disposizione che lo sancisce e che, per buona

---

dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". La definizione contenuta all'art. 4, lett. a) del D.lgs. 196/03 era, invece, la seguente: "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*".

[14] Si ricorda la definizione di dati sensibili; l'art. 4, lett. d) li definisce come "*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*".

[15] Il riferimento è all'art. 9 del Regolamento che, dopo aver sancito il divieto, elenca le seguenti deroghe:

parte, mantiene invariate (almeno sostanzialmente) le regole contenute nel d.lgs. 196/03. Di particolare interesse è il comma 4 dell'art. art. 9 in commento, il quale espressamente rimanda agli stati membri il compito, eventua-

---

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale , che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

le, di "*mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute*".

In attesa degli ulteriori sviluppi normativi, nel senso anzidetto, la vigente disciplina individua tre principali ipotesi di trattamento dei dati personali di natura sensibile. Nel primo caso, i soggetti pubblici possono trattare dati sensibili soltanto in presenza di una espressa disposizione di legge nella quale siano specificati: i tipi di dati che possono essere trattati; i tipi di operazioni eseguibili su tali dati; le finalità di rilevante interesse pubblico perseguite dai trattamenti[16]. Nella seconda ipotesi, se una disposizione di rango primario si limita a specificare la finalità di rilevante interesse pubblico, ma non individua i tipi di dati sensibili che possono essere trattati ed i tipi di operazioni che possono essere eseguite, il trattamento è consentito a condizione che i soggetti titolari provvedano ad individuare e rendere pubblici i tipi di dati e di operazioni oggetto del trattamento. L'individuazione richiesta dalla norma deve essere effettuata nel rispetto dei principi espressi dall'art. 22 del Codice[17], attraverso un atto di natura regolamentare da adottarsi previo parere conforme del Garante, *ex* art. 154, co. 1, lett. g), anche sulla base di schemi-tipo[18]. Infine, nel terzo caso, qualora un determinato trattamento di dati sensibili non sia previsto da alcuna norma di legge, i soggetti pubblici possono richiedere al Garante di individuare, tra le varie attività ad essi demandate dalla legge, quelle che perseguono "finalità di rilevante interesse pubblico" e per le quali "è conseguentemente autorizzato, ai sensi dell'art. 26, comma 2, il trattamento dei dati sensibili". Come nell'ipotesi precedente, anche in questo caso l'ente pubblico deve provvedere ad identificare e rendere pubblici i tipi di dati e di operazioni del trattamento con atto regolamentare adottato in conformità al parere espresso dal Garante[19].

---

[16] Art. 20, comma 1, D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)

[17] Secondo i principi sanciti dall'art. 22, D. Lgs. 30 giugno 2003, n. 196, nell'individuare i dati oggetto del trattamento il soggetto pubblico deve prevenire la violazione dei diritti, delle libertà fondamentali e della dignità dell'interessato. Inoltre, i soggetti pubblici possono trattare solo i dati sensibili indispensabili per svolgere le attività istituzionali che non possono essere adempiute con l'uso di dati anonimi o di natura diversa.

[18] Art. 20, comma 2, D. Lgs. 30 giugno 2003, n. 196

[19] Art. 20, comma 3, D. Lgs. 30 giugno 2003, n. 196

In via generale, in tutti i casi fin qui esaminati deve essere sempre rispettato il principio di indispensabilità, in base al quale il trattamento dei dati sensibili, quando non può essere effettuato mediante l'uso di dati anonimi, deve avere luogo solo nel caso in cui questo sia ritenuto indispensabile per svolgere le attività istituzionali.

2.1 La circolazione dei dati sanitari oltre i confini europei

Sulla base dei principi e delle regole appena illustrate, il trattamento in *cloud* di dati sensibili presenta particolari problematiche di sicurezza in caso del loro trasferimento oltre i confini europei. In base alla disciplina contenuta nel D.lgs. 196/03 la circolazione dei dati personali può avvenire sostanzialmente in due differenti modi: con la "diffusione", quando i destinatari dei dati sono indeterminati e indeterminabili, ovvero con la "comunicazione", quando avviene verso soggetti determinati. Nel primo caso, sia in ambito nazionale che europeo, sussiste un divieto generale ed assoluto di diffusione dei dati sanitari[20], mentre per i dati oggetto di comunicazione è necessario distinguere quando il trasferimento avvenga all'interno dell'Unione Europea (o dello Spazio Economico Europeo) o in territorio extra-europeo. In generale, quando la comunicazione tra soggetti determinati o la trasmissione (se effettuata dal titolare al responsabile) avviene tra soggetti determinati i dati sanitari devono circolare in forma cifrata[21].

La comunicazione di dati sanitari è già stata oggetto di approfondimento da parte del Garante *Privacy* in occasione della stesura delle Linee guida in materia di referti *on-line*, emanate con provvedimento del 25 giugno 2009[22]. Le considerazioni svolte in quella sede sono a tutti gli effetti applicabili anche nell'ambito degli scenari del *cloud*. In particolare, osservava il Garante, in caso di trasmissione dei dati tra il *server* del titolare del trattamento (la struttura sanitaria pubblica) e il *client* dell'interessato (utente o paziente), questa deve avvenire attraverso protocolli di comunicazione sicuri, basati

[20] Art. 22, comma 8, D. Lgs. 30 giugno 2003, n. 196.

[21] D.lgs. 196/03, All. b) n. 24.

[22] Il provvedimento è consultabile al seguente link http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1630271

sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (es. protocolli *https ssl – Secure Socket Layer*). Inoltre, quando sono trasmessi documenti allegati contenenti dati sanitari (come, ad esempio, il referto *on-line*) è necessario l'utilizzo di *password* o di chiavi crittografiche per l'apertura del *file*, da comunicare al destinatario tramite canali diversi da quelli usati per la trasmissione dei dati. Oltre all'obbligo di adottare tecniche idonee ad evitare l'acquisizione non autorizzata del dato durante la consultazione del documento tramite sistemi di *caching* locali o centralizzati, il Garante ha prescritto anche l'uso di idonei sistemi di autenticazione informatica (credenziali o, preferibilmente, tramite procedure di "*strong authentication*") affinché sia consentita l'individuazione sicura del destinatario della comunicazione stessa[23].

Per quanto concerne la circolazione dei dati sanitari all'interno dell'Unione Europea e dello Spazio Economico Europeo non sono richiesti particolari requisiti, mentre nel caso di circolazione verso territori *extra* UE affinché l'attività possa considerarsi lecita è necessario verificare la sussistenza di alcune condizioni[24].

In primo luogo occorre verificare il livello di adeguatezza del Paese destinatario dei dati sanitari. Con ciò si intende che le regole poste a tutela dei dati personali in vigore nel Paese extra UE siano adeguate ai livelli di protezione richiesti nell'Unione Europea e, in caso positivo, potrà procedersi al trasferimento. La valutazione in ordine al livello di adeguatezza è svolta dalla Commissione Europea, coadiuvata dalle verifiche effettuate dal Gruppo di Lavoro ex Art. 29 per la protezione dei dati dell'Unione Europea[25].

---

[23]Ad esempio, per l'invio del referto *on-line* via *e-mail* al paziente è richiesto quantomeno che si proceda alla convalida degli indirizzi *e-mail* tramite apposita procedura di verifica *on-line*.

[24] In base all'art. 45 del D.lgs. 196/03, il trasferimento dei dati da un Paese UE verso paesi terzi (non appartenenti all'UE o allo SEE, quali la Norvegia, Islanda e Liechtenstein) è vietato, anche se temporaneo (cfr. anche l'art. 25, comma 1, Dir. 95/46/CE).

[25] Attualmente i paesi con un livello di adeguatezza idoneo sono: Andorra, Argentina, Australia, Canada, Guernsey, Isola di Man, Isole Far Oer, Israele, Isola di Jersey, Nuova Zelanda, Principato di Monaco, Svizzera, Uruguay. Per gli Stati Uniti, vigeva il sistema *Safe Harbor*, che, con Decisione della Commissione Europea 2000/520/CE del 26 luglio 2000, fu definito di livello adeguato per la protezione dei dati personali trasferiti verso gli USA. Come si dirà meglio nel prosieguo, il 6 ottobre 2015, la Corte di Giustizia dell'Unione Europea ha invalidato la suddetta Decisione 2000/520/CE.

Al contrario, nel caso in cui non vi sia giudizio di adeguatezza, affinché possa essere effettuato il trasferimento dei dati sanitari occorre rispettare particolari requisiti e adottare specifiche misure ed accorgimenti. In particolare, è necessario acquisire il consenso scritto dell'interessato, che deve essere specifico e ulteriore rispetto al consenso per altre operazioni di trattamento del dato[26]. Tuttavia, non è richiesto il consenso: nell'ipotesi in cui il trasferimento "*sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato; per l'adempimento, prima della conclusione del contratto, a specifiche richieste dell'interessato; ai fini della conclusione o dell'esecuzione di un contratto stipulato a favore dell'interessato*"[27].

Il trasferimento *extra*-UE è altresì consentito, senza il consenso dell'interessato, quando è "*necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21*"[28]. Allo stesso modo, non è necessario il consenso quando il trasferimento è effettuato al fine di salvaguardare la vita o l'incolumità fisica di un terzo o dell'interessato[29].

Al di fuori delle ipotesi sopra menzionate, il trasferimento dei dati fuori dal territorio comunitario è consentito, su autorizzazione del Garante, a condizione che siano adottate particolari clausole o modelli contrattuali che offrano adeguate garanzie per l'interessato e che siano vincolanti per il destinatario dei dati da trasferire[30]. In particolare, possono essere utilizzati i modelli contrattuali *ad hoc* elaborati dal Garante, le cosiddette *Binding Corporate Rules* (*BCR*)[31], applicabili tra società appartenenti allo stesso gruppo, nel caso di multinazionali aventi sedi in Stati diversi e, infine, i modelli contrattuali elaborati dalla Commissione Europea.

---

[26] Art. 43, comma 1, lett. a), D. Lgs. 30 giugno 2003, n. 196.

[27] Art. 43, comma 1, lett. b), D. Lgs. 30 giugno 2003, n. 196

[28] Art. 43, comma 1, lett. c), D. Lgs. 30 giugno 2003, n. 196.

[29] Art. 43, comma 1, lett. d), D. Lgs. 30 giugno 2003, n. 196

[30] Art. 44, D. Lgs. 30 giugno 2003, n. 196

[31] Le *Binding Corporate Rules* sono documenti nei quali sono specificate le regole (*rules*) che disciplinano i livelli di tutela dei dati personali in modo vincolante (*binding*) per tutte le società facenti parte di un medesimo gruppo (*corporate*). L'uso delle BCR deve essere sempre autorizzato dal Garante.

2.2 La più recente disciplina europea in materia di trasferimento dei dati all'estero

Il Regolamento Privacy dedica l'intero Capo V al "*trasferimento di dati personali verso paesi terzi o organizzazioni internazionali*" confermando, in buona parte, la disciplina contenuta nel D. Lgs. 196/03.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso, innanzitutto, se la Commissione ha deciso che il paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

Diversamente, qualora manchi la valutazione di adeguatezza il titolare del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati.

Ancora, il trasferimento dei dati verso paesi terzi può anche avvenire quando vi siano norme vincolanti d'impresa che però devono essere approvate dall'Autorità di controllo purché:

a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo di imprese o gruppi di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;

c) soddisfino tutta una serie di requisiti quali l'indicazione della struttura e delle coordinate di contatto del gruppo d'imprese in questione e di ciascuno dei suoi membri; l'indicazione dei trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione di default, alla base giuridica del trattamento e al trattamen-

to di specifiche categorie di dati personali sensibili, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa; l'indicazione dei diritti dell'interessato in relazione al trattamento dei suoi dati personali e i mezzi per esercitarli ed ancora altri specificati dall'art. 47 del RGPD.

L'art. 48 del Regolamento Privacy prevede anche diverse deroghe all'applicazione dei principi generali in tema di trasferimento dei dati verso paese terzi specificati in precedenza. Varie sono le ipotesi prese in considerazione, tra le principali si annoverano i casi in cui l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate, oppure il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il responsabile del trattamento ovvero all'esecuzione di misure precontrattuali prese su istanza dell'interessato, oppure il trasferimento sia necessario per importanti motivi di interesse pubblico, oppure il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, ecc.

2.3 Trasferimento di dati personali verso gli USA: dal *Safe Harbor* al *Privacy Shield*

Il 6 ottobre 2015 la Corte di Giustizia dell'Unione Europea ha dichiarato invalida la Decisione 2000/520/CE del 26 luglio 2000, con la quale la Commissione Europea aveva riconosciuto che il sistema *Safe Harbor* garantiva un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti[32].

La sentenza è stata emessa al termine di una lunga vicenda iniziata nel 2013, quando lo studente austriaco Maximilian Schrems è opposto alla decisione del *Data Protection Commissioner* (l'Autorità Garante per la protezione dei dati personali irlandese) di non istruire la sua denuncia relativa a possibili violazioni da parte della Facebook Ireland Ltd. (sede fiscale e legale in Europa della Facebook Inc.) degli accordi di *Safe Harbor*, in quanto la stessa

[32] Art. 1, Decisione 2000/250/CE

società trasferiva i dati personali degli utenti negli Stati Uniti e li conservava nei server situati in tale Paese, così sottoponendoli così ad una potenziale attività di controllo in spregio ai principi comunitari. L'Autorità Garante irlandese, nel motivare il provvedimento di diniego, sosteneva, oltre alla carenza di prove in merito ai fatti allegati, che "*le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato*"[33].

Il provvedimento di diniego veniva impugnato dinnanzi la *High Court* irlandese la quale, ritenendo fondata la questione e considerato che essa verteva sull'attuazione del diritto dell'Unione europea, sospendeva il procedimento e sottoponeva alla Corte di Giustizia Europea due questioni pregiudiziali. In particolare, la Suprema Corte chiedeva al giudice comunitario se l'art. 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione Europea, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE, con la quale la Commissione constata che un Paese terzo assicura un livello di protezione adeguato, osti a che un'autorità di controllo di uno Stato membro (nel caso di specie, il *Data Protection Commisioner*) possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento dei propri dati personali. Questo perché tali dati sono stati trasferiti da uno Stato membro verso il sopracitato Paese terzo, quando il diritto e la prassi in vigore in quest'ultimo non assicurano un livello di protezione adeguato.

Nella sua lunga e complessa argomentazione, la Corte di Giustizia UE afferma che la decisione 200/250/CE ha, di fatto, sancito il primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti sui principi del *Safe Harbor* (approdo sicuro), in

[33] P. 29, Sent. Corte di Giustizia dell'Unione Europea, C-362/14, M. Schrems vs. Data Protection Commissioner

base al quale le organizzazioni americane autocertificate[34] che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

La Decisione 2000/250/CE è stata, quindi, ritenuta invalida dalla Corte di Giustizia UE in quanto la stessa consentiva ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti.

Alla luce della sentenza *Safe Harbor*, la Commissione Europea supportata anche dal Gruppo di Lavoro "Articolo 29", ha subito espresso la sua preoccupazione in merito allo scenario venutosi a formare, confermando la possibilità per le imprese di poter usufruire di ulteriori strumenti per il trasferimento dei dati verso Paesi terzi. Nella sua Comunicazione[35] la stessa Commissione considera di priorità fondamentale rinnovare e rafforzare il quadro per i trasferimenti di dati personali verso gli Stati Uniti affinchè sia garantita un'effettiva continuità della protezione dei dati personali dei cittadini europei quando sono trasferiti suddetto Stato e, nello stesso tempo, offrire una soluzione migliore per le imprese operanti nel commercio transatlantico.

Sul versante italiano all'indomani della pronuncia di invalidità della Corte di Giustizia UE, anche il Garante *Privacy*, con provvedimento del 22 ottobre 2015[36], ha disposto la caducazione dell'autorizzazione adottata con la deliberazione n. 36 del 10 ottobre 2001, con la quale si autorizzavano i trasferimenti effettuati in forza del sistema *Safe Harbor*. Per l'effetto, il Ga-

[34] Un'organizzazione che intende usufruire dei vantaggi del *Safe Harbor* e, quindi, ricevere dati personali da un Paese membro dell'Unione Europea, deve autocertificare l'adesione agli accordi di "approdo sicuro" al Dipartimento del Commercio statunitense. Cfr. Faq n. 6 Allegato II, Decisione 2000/250/CE.

[35] Comunicazione del 6 novembre 2015, *"Comunicazione della Commissione Europea al Parlamento Europeo e al Consiglio relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (Schrems)*", COM(2015) 566 final

[36] Il provvedimento è consultabile al seguente indirizzo: http://www.garante*privacy*.it/web/guest/home/docweb/-/docweb-display/docweb/4396484

rante italiano, dopo aver ricordato tutti gli strumenti previsti dal Codice *Privacy* per il trasferimento verso Paesi *extra*-UE[37], ha disposto il divieto per i trasferimenti di dati verso gli Stati Uniti effettuati sulla base degli accordi suddetti.

Al momento in cui si redige il presente lavoro non è stato ancora approvato, in via definitiva, il "*EU-US Privacy Shield*", che consentirà i trasferimenti di dati personali dall'Unione Europea agli Stati Uniti, in sostituzione del *Safe Habor* ma alcuni dettagli sul contenuto sono già stati pubblicati.

La Commissione Europea il 29 febbraio 2016 ha reso disponibile una bozza di decisione sull'adeguatezza del Privacy Shield ("draft adequacy decision"), contenente i principi che dovranno essere osservati da parte delle aziende statunitensi interessate ad importare dati personali dall'Europa e gli impegni del governo statunitense sull'applicazione dell'accordo, con particolare riguardo alle limitazioni in materia di accesso ai dati personali da parte delle autorità pubbliche di sicurezza.

In base alla bozza pubblicata, si prevede che le aziende agiranno sotto il controllo del *Department of Commerce* e dovranno verificare che gli obblighi relativi ai diritti individuali siano rispettati anche da aziende a cui, evetualmente, i dati vengano successivamente trasferiti. È, altresì, previsto un monitoraggio periodico del regolare funzionamento del nuovo regime, consistente in una revisione congiunta annuale, condotta dalla Commissione Europea e dal *Department of Commerce*, alla quale prenderanno parte esperti nazionali di intelligence degli Stati Uniti e delle Autorità di protezione dei dati.

[37] Nella parte in premessa del provvedimento, il Garante ricorda come i trasferimenti dei dati personali verso un Paese non appartenente all'Unione europea possono essere effettuati sulla base di ulteriori presupposti di liceità, così come previsto negli artt. 43 ("Trasferimenti consentiti in Paesi terzi") e 44 ("Altri trasferimenti consentiti") del Codice. In particolare, con riferimento all'art. 43, i dati possono essere trasferiti sulla base di una delle deroghe di cui al comma 1 e, nello specifico, qualora gli interessati abbiano espresso liberamente il loro consenso specifico e informato. Inoltre, con riferimento all'art. 44, i trasferimenti possono essere effettuati mediante l'utilizzo delle clausole contrattuali tipo (c.d. *standard contractual clauses*) autorizzate con provvedimento del Garante, ovvero in ragione dell'avvenuta adozione, nell'ambito di società appartenenti a un medesimo gruppo, delle *Binding Corporate Rules*. Infine, i trasferimenti sono consentiti su specifica autorizzazione dell'Autorità Garante sulla base di adeguate garanzie per i diritti dell'interessato.

Altro punto interessante del *Privacy Shield* è rappresentato dall'assicurazione, da parte degli Stati Uniti, che saranno previsti limiti chiari alla possibilità per le autorità di pubblica sicurezza di accedere ai dati personali e che non ci saranno attività di monitoraggio indiscriminato e non proporzionale. In tal senso, i cittadini europei che riterranno i propri diritti violati negli Stati Uniti potranno rivolgersi direttamente alle aziende, che avranno l'obbligo di trattare i reclami entro 45 giorni, ovvero alle Autorità Garanti del proprio Paese, nonché ad un difensore civico ("*Ombudsperson*"), qualora sospettino che i propri dati personali siano stati illegalmente utilizzati dalle Autorità di intelligence statunitensi.

Il 13 aprile 2016 il gruppo ex Articolo 29, che riunisce i garanti europei, ha espresso un parere sulla bozza del *Privacy Shield* affermando che sono necessari ancora dei miglioramenti in quanto il testo, di fatto, permette ancora la sorveglianza di massa indiscriminata e affida pochi poteri e molto vaghi alla figura del mediatore che dovrebbe tutelare i dati degli europei una volta trasferiti oltreoceano. Inoltre, si pone la necessità di sottoporlo a revisione anche alla luce dell'approvazione del nuovo Regolamento Europeo in tema di protezione dei dati personali.

Per il garante francese e presidente del gruppo Art. 29, Isabelle Falque-Pierrotin, il *Privacy Shield* rappresenta certo un passo avanti rispetto al Safe Harbour ma, afferma: "*è inaccettabile che nel testo permanga la possibilità di una raccolta di dati massiccia e indiscriminata*"[38].

Il parere del Gruppo dei Garanti Europei non è vincolante ma ha certamente un peso rilevante in quanto in quanto, a prescindere dalla presenza di un accordo transatlantico, i garanti nazionali, come sancito anche dalla Corte di Giustizia europea, hanno facoltà di indagare e sospendere il trasferimento dei dati se ritengono che i diritti degli europei non siano adeguatamente protetti.

Da ultimo, il 26 maggio 2016, il Parlamento Europeo ha approvato una risoluzione non legislativa, con la quale ha chiesto alla Commissione Europea di continuare le negoziazioni con gli Stati Uniti al fine di rimediare alle rilevate carenze del *Privacy Shield*, ossia: l'accesso da parte delle autorità di pubblica sicurezza ai dati trasferiti, la complessità del meccanismo di ricor-

[38] Il video con la relazione sul *privacy shield* è disponibile al seguente link https://scic.ec.europa.eu/streaming/article-29-working-party

so, la forte carenza di poteri effettivi in capo alla nuova figura del Mediatore nel Dipartimento di Stato, la possibilità di raccogliere grandi quantità di dati spesso contrastante con i principi di necessità e proporzionalità, nonché la generale necessità di valutare l'adeguatezza del Privacy Shield alle nuove disposizioni del Regolamento UE 679/2016.

Infine, anche il Garante Europeo per la privacy ha espresso le proprie preoccupazioni rilevando il rischio, anche per il nuovo accordo, di invalidazione da parte della Corte di Giustizia UE.

L'approvazione del testo definitivo del Privacy Shield era orginiariamente prevista per la fine di giugno 2016, termine che potrebbe essere differito a causa delle molteplici osservazioni sopraccitate, di cui, non potrà non tenersi conto nella stesura del testo definitivo.

2.4 Difficoltà di inquadramento soggettivo

Merita una trattazione a sé stante, anche alla luce delle più recenti novità normative[39] già citate, un ulteriore aspetto critico del *cloud computing*, legato all'inquadramento delle figure soggettive codificate sul modello responsabile/titolare del trattamento.

Nonostante il recente intervento normativo (e nell'incertezza della sua portata risolutiva), la questione rimane attuale in quanto la nuova disciplina (Art. 99, comma 2, RGPD) si applicherà a decorrere dal 25 maggio 2018.

Il rapporto giuridico tra l'utente (Pubblica Amministrazione) e il *cloud provider*, alla luce delle definizioni presenti nel D. Lgs. 196/2003, vede certamente il primo quale titolare del trattamento, mentre il secondo dovrebbe rivestire il ruolo di responsabile esterno del trattamento. Il condizionale è d'obbligo (non dal punto di vista normativo) perché una tale configurazione non risponde pienamente alle caratteristiche effettive del rapporto sussistente tra i due soggetti. L'ente fruitore, infatti, titolare del trattamento secondo il Codice *Privacy*, dovrebbe costantemente accertare l'affidabilità e la competenza del responsabile esterno, oltre che adempiere agli obblighi organizzativi e gestionali di implementazione e controllo delle misure di sicurezza che, in realtà, sono di competenza del *provider*.

[39] Regolamento generale sulla protezione dei dati.

Posto che le categorie previste dall'art. 4 del D. Lgs. 196/2003 non sono sufficienti ad inquadrare un tale rapporto, è necessario riferirsi direttamente alle figure, elaborate nella direttiva madre, del *data controller* (colui che determina le finalità e gli strumenti del trattamento) e del *data processor* (corrispondente all'incaricato[40], al quale compete l'elaborazione dei dati personali per conto del *data controller*).

Per una corretta classificazione dei ruoli è opportuno fare riferimento al rapporto sostanziale tra le parti che prevale sempre sulla qualificazione giuridica convenzionalmente stabilita dalle stesse nel contratto di fornitura dei servizi di *cloud computing*. La gran parte dei contratti stipulati per la fornitura di servizi di *cloud* standardizzati[41] contengono clausole generali accettate, per adesione, dal cliente; di fatto, quindi, il *cloud provider* si colloca in una posizione dominante rispetto al fruitore del servizio, il quale non è nelle condizioni di poter negoziare le clausole a lui meno favorevoli.

Come già sottolineato, nei contratti di *cloud* ogni decisione relativa alle misure di sicurezza da adottare e alla configurazione tecnologica dei sistemi è di esclusiva competenza del *provider*. L'Amministrazione sanitaria, benché sia titolare del trattamento, può verificare l'esatta esecuzione delle prestazioni in conformità con quanto previsto dal contratto, ma non può esercitare alcun potere di controllo sugli aspetti suddetti.

La sostanza del rapporto, quindi, vede entrambi i soggetti conservare una piena libertà decisionale in merito alle modalità del trattamento; ragion per cui sarebbe più coerente inquadrare sia il cliente che il fornitore *cloud* come titolari del trattamento e in tale direzione sembra essersi mosso il legislatore europeo con il neonato Regolamento (UE) 2016/679 generale sulla protezione dei dati, che introduce la figura del contitolare[42] ogniqualvolta

---

[40] Il D.lgs. 196/03 considera incaricato colui che materialmente opera sui dati personali, seguendo le istruzioni del titolare o del responsabile. Sul tema si veda S. SICA, sub art. 1-6, in *La nuova disciplina della privacy, Commento al D.lgs. 30 giugno 2003, n. 196*, a cura di S. SICA E P. STANZIONE, Bologna 2005, p.14.

[41] Servizi progettati sul modello del cliente tipo, offerti ad una generica e indeterminata categoria di destinatari.

[42] L'Art. 26 del Regolamento generale sulla protezione dei dati, dispone quanto segue: "*Contitolari del trattamento 1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare*

"*due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*".

La novità citata, però, potrebbe non essere la soluzione al problema del rapporto tra *cloud provider* e Amministrazione sanitaria (o altra Amministrazione fruitrice, sia essa pubblica o privata) in quanto il fornitore del servizio partecipa (e non deve partecipare) alla definizione delle finalità di trattamento. Ammettere ciò, significherebbe licenziare un'ingerenza che non appartiene (e non deve appartenere) ai rapporti quivi contemplati, in particolare se il settore d'interesse riguarda Amministrazioni Pubbliche cui compete il trattamento di dati sensibili.

In attesa di conoscere gli sviluppi interpretativi sulla portata applicativa dell'art. 26 del Regolamento Privacy, si ritiene che non vi sarebbe stato alcun dubbio sull'applicabilità di tale disposizione al rapporto tra *cloud provider* e Amministrazione sanitaria se il ruolo del contitolare fosse stato circoscritto alla determinazione congiunta dei mezzi del trattamento, e non anche delle finalità. Il ruolo più appropriato per il *cloud provider* rimane quello della "titolarità supplementare"[43], già contemplata per i fornitori di servizi di telecomunicazioni, ove il fornitore del servizio ha una titolarità limitata al "funzionamento del servizio". Ma questa non è stata la scelta del legislatore europeo.

Peraltro, l'introduzione dei "contitolari del trattamento", sostanzialmente, non rappresenta una novità ma esclusivamente una esplicitazione di quanto già contenuto (tanto nella vecchia, che nella nuova disciplina) nella definizione di "titolare del trattamento"[44]. La reale portata innovativa

---

riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati. 2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. 3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento".

[43] Cfr. Direttiva 95/46/CE, considerando n. 47.

[44] L'art. 4, n. 7) del Regolamento generale sulla protezione dei dati definisce la figura del "titolare del trattamento", specificando che il ruolo può essere svolto "*singolarmente o insieme*

dell'art. 26 è costituita dalla previsione formale dell'"accordo interno" per la definizione delle "*rispettive responsabilità [...] con particolare riguardo all'esercizio dei diritti dell'interessato*".

É doveroso, ancora una volta, evidenziare che le difficoltà di inquadramento quivi rappresentate appartengono soltanto ai rapporti negoziali in cui il *cloud provider* ha una forza e autonomia tali che impediscono una sua etero-determinazione nei confronti del fruitore del servizio (Pubblica Amministrazione sanitaria). In caso contrario, il binomio titolare/responsabile non comporta alcuna difficoltà di inquadramento dei protagonisti coinvolti.

Al di là del rapporto tra fruitore e fornitore del servizio, la contitolarità è presente nel momento in cui più Amministrazioni sanitarie svolgono un trattamento congiunto sui dati conservati in una medesima piattaforma. In tali casi (come avviene, ad esempio, in ambito FSE) è indubbio che "*più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*"[45].

2.5 Contromisure per la sicurezza dei dati personali: i parametri per la scelta del fornitore e l'introduzione della certificazione

Quando i dati contenuti nella nuvola sono di natura sensibile le criticità si trasformano in veri e propri rischi. Tale consapevolezza è stata esternalizzata anche dal Garante *privacy* italiano, il quale, nel già citato documento intitolato "*Cloud computing. Proteggere i dati per non cadere dalle nuvole*", rileva che, l'esternalizzazione del trattamento dei dati, mediante l'uso di grandi elaboratori gestiti da fornitori privati (i cosiddetti *cloud providers*), impone alla Pubblica Amministrazione di valutare con assoluta attenzione anche ogni possibile insidia legata a questo nuovo modello di *e-Government*.

La migrazione dei dati al di fuori dei sistemi locali dell'Amministrazione sanitaria crea, in capo al fornitore del servizio, un ruolo centrale in ordine alla sicurezza dei dati e, quindi, all'adozione delle misure necessarie a ga-

---

ad altri". Tale inciso, già presente nel D.lgs. 196/03, rappresenta l'introduzione implicita della figura del contitolare, sconosciuta sotto la vigenza della L. 675/96.

[45] Art. 26 del Regolamento generale sulla protezione dei dati.

rantirla. In tal senso, il Garante *privacy*, nel Provvedimento sopraccitato, afferma che:

"*• l'utente, affidando i dati ai sistemi di un fornitore remoto, ne perde il controllo diretto ed esclusivo; la riservatezza e la disponibilità delle informazioni allocate sulla nuvola certamente dipendono anche dai meccanismi di sicurezza adottati dal* service provider*;*

• il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri service provider*, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati;*

• il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali quali, ad esempio, guasti, impedendo l'accessibilità temporanea ai dati in esso conservati;

• le cloud *sono sistemi e infrastrutture condivise basate sul concetto di risorse noleggiate a un'utenza multipla e mutevole; i fornitori, infatti, custodiscono dati di singoli e di organizzazioni diverse che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza;*

• la conservazione dei dati in luoghi geografici differenti ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra l'utente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati;

• l'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la transizione di dati e documenti da un sistema cloud *ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi* cloud *di fornitori differenti, ponendone quindi a rischio la portabilità o l'interoperabilità dei dati*".

Rinviando a quanto detto nel paragrafo che precede, sul ruolo (di responsabile o di contitolare) assunto dal *cloud provider*, i rischi per la sicurezza dei dati impongono all'Amministrazione sanitaria di scegliere il fornitore tra i soggetti dotati di solida esperienza nel trattamento dei dati persona-

li compreso il profilo della sicurezza. Ne consegue, come osservato da autorevole dottrina[46], che l'Amministrazione dovrà selezionare con estrema cura il fornitore, privilegiando quello:

" • dotato di certificazioni di settore;

• che detenga una reale stabilità societaria (elemento che potrebbe aiutare nella comprensione della sua affidabilità);

*• che si impegna al mantenimento di specifici livelli di servizio (*service level agreement*)*

• che utilizzi modalità di archiviazione e trasmissione sicure, tenuto conto delle prescrizioni in materia di sicurezza di cui agli art. 31-34 del D.lgs. 196/03[47], mediante tecniche crittografiche (specialmente quando i dati sono particolarmente delicati, come in caso di dati sanitari), accompagnate da solidi meccanismi di identificazione dei soggetti autorizzati all'accesso;

• che consenta la portabilità dei dati, con procedure semplificate, rispettando l'architettura di fascicoli e cartelle coinvolti, come anche le codifiche applicate ai dati (preferibilmente codifiche internazionali come H.L.7)e l'eventuale formato aperto prescelto".

Tra i criteri sopraelencati, tutti fondamentali per la scelta del fornitore, il nuovo Regolamento (UE) 2016/679, introduce, tra le varie novità, proprio la

[46] M. MANCARELLA, "e-*Health e diritti, l'apporto dell'informatica giuridica, 2012, p. 223-224.*;

[47] Anche il Regolamento (UE) 2016/679 contiene un espresso riferimento alle misure di sicurezza disponendo che il titolare del trattamento debba implementare misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è compiuto nel rispetto della disciplina posta a tutela dei dati personali (cosiddetto principio di *accountability*). In particolare l'art. 32, a proposito della sicurezza del trattamento, dispone che tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e l'incaricato del trattamento devono "*mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

certificazione di settore. L'articolo 42, rubricato "certificazione", al comma 1, conferisce agli Stati membri il compito di incoraggiare "*l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati*" allo scopo di dimostrare la conformità dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento alla normativa. Si tratta di una certificazione volontaria, che non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo.

La certificazione è rilasciata dagli organismi di certificazione o dall'Autorità di controllo[48]oppure dal Comitato europeo per la protezione dei dati[49]. Ove i criteri siano approvati dal Comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.

---

[48] L'art. 51 del Regolamento prevede che ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Si tratta in altri termini della nostro Garante per la protezione dei dati personali.

Ogni autorità di controllo contribuisce alla coerente applicazione del Regolamento in tutta l'Unione. A tale scopo le autorità di controllo cooperano tra loro e con la Commissione. Inoltre l'autorità di controllo agisce in piena indipendenza nell'adempimento dei compiti e nell'esercizio dei poteri che le sono stati conferiti conformemente al Regolamento.

Tra i numerosi poteri previsti dal Regolamento, all'autorità di controllo, in materia di certificazioni, compete di:

" - *revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiunger eall'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti* (art. 58, comma 2, lett. h)

- *accreditare gli organismi di certificazione a norma dell'articolo 43soddisfatti* (art. 58, comma 3, lett. e);

- *rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5*" (art. 58, comma 3, lett. f).

[49] L'art. 68 prevede il Comitato europeo per la protezione dei dati che è istituito come organismo dell'Unione europea ed è dotato di personalità giuridica. Il Comitato europeo per la protezione dei dati è rappresentato dal suo presidente. Il comitato europeo per la protezione dei dati è composto dal responsabile di un'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti. Nell'adempimento dei suoi compiti o nell'esercizio dei suoi poteri, il Comitato europeo per la protezione dei dati opera con indipendenza.

Tra gli innumerevoli compiti del Comitato europeo a norma dell'art. 70, alcuni sono dedicati alle certificazioni:

Il titolare del trattamento che si sottopone alla procedura suddetta deve ovviamente fornire all'organismo di certificazione o, se del caso, all'Autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a conseguire la certificazione.

La certificazione ottenuta ha una durata limitata nel tempo, fissata nel termine massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. Può essere, altresì, revocata dagli stessi organismi di certificazione o dall'Autorità di controllo competente, qualora non siano più soddisfatti i requisiti per la certificazione.

Per quanto concerne gli organismi di certificazione, la loro disciplina è contenuta nell'art. 43 del RGPD, il quale fatti salvi i compiti e i poteri dell'Autorità di controllo competente, prevede che essi, se in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilascino e rinnovino la certificazione, dopo averne informato la medesima Autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri (*revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione […], oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti*)[50].

Gli organismi di certificazione devono essere accreditati, singolarmente o contemporaneamente:

a) dall'autorità di controllo;

b) dall'organismo nazionale di accreditamento conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo.

"*n) incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ai sensi degli articoli 40 e 42;*

o) effettua l'accreditamento di organismi di certificazione e il suo riesame periodico anorma dell'articolo 43 e tiene un registro pubblico di organismi accreditati a norma dell'articolo 43, paragrafo 6, e dei titolari o responsabili del trattamento accreditati,stabiliti in paesi terzi a norma dell'articolo 42, paragrafo 7;

p) specifica i requisiti di cui all'articolo 43, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione ai sensi dell'articolo 42;

q) fornisce alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 43, paragrafo 8".

[50] Art. 58, comma 2, lett. h), Regolamento Privacy

L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti previsti dal Regolamento.

Va inoltre precisato che gli organismi di certificazione di cui sopra sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità dei trattamenti eseguiti al Regolamento (UE) 2016/679.

2.6 La norma ISO 27018: lo *standard* della "nuvola"

Ancor prima dell'introduzione delle recenti novità appena illustrate in materia di certificazione, nel luglio del 2014, l'ente internazionale ISO ha pubblicato lo *standard* 27018 specificamente elaborato per i fornitori di servizi di *cloud computing*. Si tratta di un *set* di regole costruito sugli *standard* ISO 27001[51] e 27002[52] per garantire il rispetto dei principi e delle norme privacy dettate dalla Direttiva 95/46/CE, da parte dei *providers* di *public cloud* che decidano di certificarsi. La nuova norma fornisce una risposta concreta, in chiave "*data protection by design and by default*"[53] – alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del *cloud* pubblico.

L'impiego di servizi di *cloud*, come illustrati nella parte terza del presente lavoro, è divenuto una strada obbligata per un grande numero non solo di imprese commerciali, ma anche di enti pubblici. A fronte di tale diffusione, da qualche anno le autorità garanti dei dati personali, riunite nel Gruppo ex

[51] Il 27001 è uno *standard* rivolto alle organizzazioni che intendano adottare una *policy* di gestione dei rischi dei propri sistemi IT (*Information Security Management System*, ISMS). Esso stabilisce una serie di requisiti generici che i possessori della certificazione sono chiamati ad avere affinché le informazioni contenute nei propri sistemi IT possano essere ritenute al sicuro, ma non distingue gli enti certificati né per natura, né per dimensione.

[52] Il 27002 è uno *standard* dedicato all'analisi dei rischi specifici dei sistemi IT. Il 27018 parte da esso e ad esso rinvia, per quanto non specificamente disposto.

[53] Il concetto di "*data protection by design and by default*" (già noto come "*privacy by design and by default*", successivamente introdotto nel Regolamento (UE) 2016/679, sarà approfondito nel paragrafo successivo.

Art. 29, hanno messo in guardia i fruitori del *cloud computing* contro i rischi di scarsa trasparenza sulle modalità e sui soggetti che processano i dati, nonché di perdita di controllo sui dati personali medesimi. In tale direzione, nel più volte citato Parere 5/2012 sul *cloud computing* si legge "*affidando dati personali a sistemi gestiti da un fornitore di servizi* cloud, *i clienti rischiano di perdere il controllo esclusivo dei dati e di non poter prendere le misure tecniche e organizzative necessarie per garantire la disponibilità, l'integrità, la riservatezza, la trasparenza, l'isolamento , la portabilità dei dati e la possibilità di intervento sugli stessi*".

Nel medesimo parere, si afferma che "*la verifica o la certificazione indipendente effettuata da un terzo affidabile può essere uno strumento credibile per i fornitori* cloud *per dimostrare la conformità con gli obblighi posti a loro carico*».

Le misure introdotte dallo *standard* ISO 27018 si inseriscono in uno scenario di rischio, stabilendo procedure e controlli attraverso cui i *providers* di servizi *cloud* garantiscono il rispetto della direttiva europea sul trattamento dei dati personali e, nel contempo, rassicurando i potenziali acquirenti circa la possibilità di controllare, sempre e in piena trasparenza, il processo subito dai dati personali entro i sistemi *cloud* del *provider*. La certificazione ISO 27108 va dunque qualificata come una *best practice* sintomatica della credibilità e reputazione dei fornitori *cloud* che se ne doteranno, in quanto sembra poter dare piena prova della conformità del *provider* certificato con i principi *privacy* sanciti dalla direttiva: consente di verificare la posizione del venditore rispetto agli obblighi *privacy*, sia esaminando i documenti forniti da un certificatore terzo a seguito di *audit* 27001, oppure rivedendo la lettera periodica con cui l'ISO garantisce che gli enti certificati hanno implementato tutti i controlli previsti dallo *standard* 27018.

Venendo ora al dettaglio, le misure contenute nell'ISO 27018 garantiscono che:

- l'interessato possa esercitare i propri diritti nei confronti del Titolare, nonostante i suoi dati siano processati da un responsabile esterno e in una nuvola informatica (è infatti un obbligo preciso del fornitore, ai sensi dello standard, offrire al Titolare del trattamento, suo cliente, dei *tools* appropriati che assicurino l'esercizio dei diritti da parte dei soggetti cui i dati si riferiscono);

- i mezzi del trattamento siano esattamente rispondenti a quelli indicati nella *policy* resa nota all'acquirente dei servizi fin dall'inizio, con esplicita previsione che, nel caso un mutamento di mezzi si rendesse necessario per ragioni tecniche, il cliente ne sia prontamente informato e abbia la facoltà di opporsi oppure uscire dal contratto;
- i dati personali in cloud non siano trattati per ragioni di *marketing*[54] diretto o pubblicitarie, a meno che non vi sia l'esplicito consenso dell'interessato, ma in ogni caso ciò non può mai costituire una precondizione posta dal fornitore al cliente per la fornitura del servizio.
- i clienti conoscano fin da subito i nomi degli eventuali *subprocessors*, e il posto in cui essi sono stabiliti, con diritto di opporsi ad eventuali modifiche nella catena dei subfornitori, ovvero dei paesi di loro stabilimento (può anche essere prevista l'opzione di risolvere il contratto a fronte di tali mutamenti);
- i clienti ricevano notizia tempestiva delle violazioni di dati personali (*data breaches*)[55], al fine di poter a loro volta darne notizia

[54] Vieta al fornitore di servizi *cloud* non soltanto di trattare i dati ad esso affidati per ragioni di *marketing* non previamente accettate dagli interessati – condotta che di suo sarebbe comunque illegale nel contesto giuridico europeo – bensì esige che il fornitore non condizioni l'erogazione dei servizi *cloud* alla possibilità di *marketing* diretto nei confronti degli interessati, i cui dati siano trattati dal cliente-titolare per proprie legittime finalità. Questa regola incorpora i principi di finalità e proporzionalità del trattamento sanciti dal diritto europeo fin dal suo livello più alto, quello della Carta dei Diritti Fondamentali, perché da un lato richiede che i dati personali non siano trattati per fini diversi da quelli per i quali siano stati raccolti, e dall'altro frappone un ostacolo al trattamento non necessario di dati personali da parte del *provider* di servizi *cloud*.

[55] Si tratta dell'obbligo per i fornitori di servizi *cloud* di notificare i cosiddetti *data breaches* ai propri clienti. La norma ha anticipato il contenuto degli articoli 33 e 34 del Regolamento *Privacy*, estendendo per tutti i titolari del trattamento l'obbligo di avvertire le autorità di controllo e gli interessati in caso di violazioni dei dati personali da essi trattati, che la pregressa normativa europea (Direttiva 2002/58/CE sulla *privacy* nelle comunicazioni elettroniche) imponeva soltanto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico. Nello specifico, l'art. 33 del Regolamento dispone che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti

alle autorità di controllo (e agli interessati) nei tempi previsti dalla legge;

- siano disciplinate le modalità di restituzione dei dati personali al cliente una volta terminato il contratto (cd. *transfer back*).
- i servizi *cloud* siano soggetti a verifiche periodiche di conformità agli *standard* di sicurezza, di cui sia fornita evidenza ai clienti;

---

un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata.
Tale notifica deve come minimo:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati in questione;
b) indicare il nome e le coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
e) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
Il titolare del trattamento documenta qualsiasi violazione dei dati personali,incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo.
L'art. 34, invece, prevede un'altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all'interessato.
Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
La predetta comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'art. 33.
Non è richiesta la comunicazione all'interessato di cui sopra se:
"*a) il responsabile del trattamento ha utilizzato le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura, oppure*
b) il responsabile del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1, oppure
c) detta comunicazione richiederebbe sforzi sproporzionati. In una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

- tutto il personale addetto al trattamento di dati personali sia vincolato da patti di riservatezza (*not disclosure agreements*) e riceva adeguata formazione.

Le norme appena illustrate allineano il trattamento di dati personali nella "nuvola" ai più alti *standard* e principi normativi in materia. Esse forniscono un rimedio alle problematiche contrattuali più diffuse in fatto di servizi *cloud*, caratterizzati spesso da offerte e condizioni predisposte dai fornitori e non negoziabili dai clienti, spesso incompatibili con le obbligazioni che il cliente di servizi *cloud* assume quale Titolare del trattamento per effetto della legge *privacy* applicabile. Aderendo all'ISO 27018, i fornitori *cloud* segnalano ai (potenziali) clienti la propria disponibilità ad incorporare i valori della normativa europea di protezione dei dati personali, e ciò testimonia l'assoluta utilità di questo *standard* anche rispetto alla strategia delineata dalla Commissione Europea nella Comunicazione "*Unleashing the potential of cloud computing in Europe*", nella quale l'esecutivo comunitario si poneva l'obiettivo di sviluppare uno standard europeo per la certificazione dell'offerta di servizi *cloud* in Europa. ISO 27018 non è ovviamente il prodotto finale di quella strategia, ma ad essa fornirà un termine di comparazione di grande qualità, per la robustezza e il valore delle sue norme.

Va comunque precisato che l'adesione allo *standard* ISO 27018 da parte di un *provider* non si traduce, necessariamente, in una trasposizione delle sue clausole in sede contrattuale: essa rimane infatti affidata alla libertà delle parti. Tuttavia, per quanto una tale trasposizione non possa inferirsi automaticamente, ISO 27018 rappresenta per i clienti *cloud* un'ottima "*checklist*" in fase acquisto dei servizi *cloud*, a cui fare riferimento per un raffronto puntuale con la normativa primaria *privacy* applicabile al *provider* e una valutazione circa la sua "ingaggiabilità".

2.7 *Data protection by design and by default*

I principi della "*data protection by design and by default*" sono stati codificati con l'art. 25 del Regolamento (UE) 2016/679 rubricato "*protezione*

dei dati fin dalla progettazione e protezione per impostazione predefinita"[56]. Con la loro introduzione si rafforza la tutela dei diritti e delle libertà degli interessati in quanto, fin dal momento della progettazione, è necessario adottare adeguate misure tecniche e organizzative che garantiscano il rispetto della disciplina di protezione dei dati personali.

L'art. 25 del Regolamento Privacy è espressione del principio di necessità, già contenuto nell'art. 3 del D.lgs. 196/03, da intendere nella sua duplice valenza di necessità di ricorrere all'utilizzo del dato personale solo in casi estremi, da una parte, e necessità anche di strutturare i servizi che utilizzano nuove tecnologie in modo tale da garantire il rispetto della riservatezza degli utenti, dall'altra.

Non si tratta, però, di concetti completamente nuovi, la "*data protection by design and by default*" può essere, infatti, definita l'evoluzione delle tradizionali PET (*Privacy Enhancing Technologies*)[57] al passo con l'evoluzione

[56] È nella versione ufficiale in lingua inglese dell'art. 25 Regolamento (UE) 2016/679 che la già nota "*privacy by design and by default*" è stata codificata come "*data protection by design and by default*".

[57] Con "*Privacy Enhancing Technologies*" ci si riferisce all'insieme di strumenti, non particolarmente invasivi della sfera privata, attraverso cui modellare i sistemi informativi. I principi chiave su cui si basano le "*Privacy Enhancing Technology*" sono essenzialmente tre: a) minimizzazione di raccolta, di utilizzo, di divulgazione e di conservazione dei dati identificativi dei pazienti; b) partecipazione e coinvolgimento attivi degli utenti, assicurati, tra l'altro, con l'esercizio di poteri di controllo durante il ciclo di vita dei dati personali trattati; c) maggiore sicurezza delle informazioni sensibili, sia sotto il profilo del diritto alla riservatezza sia sotto il profilo dell'integrità dei dati, ottenuta attraverso tecniche di anonimizzazione e di de-identificazione delle informazioni sensibili (contenute nello standard ISO/IEC 15408:1999, dedicato alla definizione dei "*Common Criteria*" per la valutazione della sicurezza dei sistemi informativi,). Per approfondimenti sulle "*Privacy Enhancing Technologies*" si vedano, tra gli altri: LONDON ECONOMICS, *Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security*, London, 2010, pp. 238; D. MARTIN, A. SERJANTOV (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop, PET 2004*, Toronto, May 2004, Berlin, 2004; ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY - COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, *Working Party on Information Security and Privacy. Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 2002, pp. 29; J. BORKING, C. RAAB, *Laws, PETs and Other Technologies for Privacy Protection*, Refereed Article, 2001 (1), The Journal of Information, Law and Technology, http://elj.warwick.ac.uk/jilt/01-1/borking.html ; O. TETTERO, *Intrinsic*

della tecnologia e, in particolare, delle comunicazioni elettroniche. L'espressione PET comparve, per la prima volta nel *report* dal titolo "*Privacy-enhancing technologies: the path to anonymty*" pubblicato nel 1995 dalla "*Dutch Registratierkamer*"[58] in collaborazione con il "*Information and Privacy Commissioner of Ontario*"[59]: uno studio volto a dedicato all'uso della tecnologia come strumento per contenere gli abusi di dati personali dei consumatori, attraverso limitazioni d'uso e di trattamento[60].

Information Security: Embedding Security Issues in the Design Process of Telematics Systems, Technical Report 6, Telematica Instituut, Enschede, The Netherlands, 2000.

[58] Autorità garante per la protezione dei dati personali olandese.

[59] Organismo indipendente che, dal 1988, sostiene e promuove il tema della protezione dei dati personali in Ontario (Canada).

[60] Nel periodo successivo alla sua prima elaborazione, il concetto di *Privacy-Enhancing Technology* si è evoluto in quello di "*PETs Plus*". In tal senso, Ann Cavoukian ("the Information and Privacy Commissioner of Ontario"), ha individuato la novità principale legata allo sviluppo di sistemi *ICT* nella realizzazione di veri e propri modelli inclusivi, in cui tutela dei dati personali del singolo utente ed interessi economici non siano antitetici ("*positive-sum paradigm*":). Così la protezione degli utenti può addirittura migliorare la sicurezza dei mercati, con beneficio per tutti i soggetti coinvolti e non soltanto dei consumatori individualmente considerati. La Commissaria dell'Ontario ha ritenuto essenziale valorizzare la funzione che le infrastrutture hanno nella tutela dei dati, anche, sensibili, di conseguenza ha ritenuto di importanza centrale la crescente implementazione di profili tecnici, che garantiscano l'efficienza e l'efficacia delle nuove tecnologie in termini di sicurezza e protezione dei dati personali. Su questi aspetti, si vedano, le seguenti fonti: CAVOUKIAN, A. *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, 2009, consultabile su http://www.privacybydesign.ca/index.php /paper/moving-forward-frompets-to-pets-plus-the-time-for-change-is-now/; CAVOUKIAN, A. *Privacy by Design. The 7 Foundational Principles*, Toronto, 2009, consultabile su http://www. privacybydesign.ca/index.php/about-pbd/7-foundationalprinciples/; CAVOUKIAN, A. e EL EMAM, K., *A Positive-Sum Paradigm in Action in the Health Sector*, 2010, consultabile su http://www.ipc.on.ca/English/Resources/Discussion-Papers/DiscussioPapersSummary/?id=943; CAVOUKIAN, A., *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, 2009, consultabile su http://www.privacybydesign.ca/index.php/paper/moving-forward-frompets- to-pets-plus-the-time-for-change-is-now/; CAVOUKIAN, A., *Privacy by Design … Take the Challenge*, 2009, consultabile su http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=856. CAVOUKIAN, A., *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, 2010, consultabile su http://www.privacybydesign.ca/index.php/paper/implementation-andmapping-of-fair-information-practices/. CAVOUKIAN, A., *Privacy by Design and the Promise of SmartData*, 2012, in HARVEY, I., CAVOUKIAN, A., TOMKO, G., BORRETT, D., KWAN, H. E HATZINAKOS, D. (eds.), *SmartData: Privacy Meets Evolutionary Robotics*, New York, Springer; CAVOUKIAN, A., *Privacy by Design : Leadership, Methods, and Results*, 2013, in

Design e *default*, anche se strettamente connessi, hanno una valenza differente: il primo è da intendere rivolto direttamente ai dati personali, o meglio, al ciclo di vita degli stessi in connessione alla tecnologia, dal principio alla fine (progettazione, distribuzione, utilizzo e eliminazione finale); la "*data protection by default*", invece, riguarda i servizi e i prodotti, che devono essere impostati con tutela della vita privata e, quindi, devono rispettare i principi generali della protezione dei dati, come, ad esempio, la minimizzazione e la limitazione delle finalità.

Considerando i tradizionali ambiti nei quali assume rilievo la "*data protection by design e by default*", i tre principali sono:

1) la tecnologia dell'informazione (*IT systems*);

2) le pratiche commerciali responsabili (*accountable business practices*);

3) la progettazione delle strutture (*physical design and infrastructure*).

Con riferimento al primo dei tre ambiti considerati, va rilevato che la tecnologia è da inquadrare come ausilio per la riduzione dei rischi legati al trattamento dei dati personali e non come una minaccia per gli stessi.

Anche per le pratiche commerciali responsabili, la "*data protection by design e by default*" non va interpretata come un onere, un costo che appesantisce l'attività imprenditoriale ma, al contrario, come un vantaggio per una migliore competitività.

L'effetto positivo, infine, deve contaminare anche la fase di progettazione delle strutture, soprattutto in tutti i casi in cui i dati personali subiscono un'esposizione in aree pubbliche progettate, senza una valutazione in termini di privacy: si pensi, ad esempio, alle sale d'attesa degli ospedali o degli uffici, ove si rischia l'illecita divulgazione delle informazioni personali.

Con la codificazione di tali principi, viene espressamente imposto, al titolare del trattamento, di mettere in atto adeguate misure e procedure tecniche e organizzative (tenuto conto dell'evoluzione tecnica e dei costi di attuazione) in modo tale che il trattamento sia conforme al Regolamento e assicuri la tutela dei diritti dell'interessato. In particolare, il titolare del trattamento (ferma la facoltà di scelta dell'interessato relativamente al trattamento dei

---

GUTWIRTH, S., LEENES, R., DE HERT, P. E POULLET, Y. (eds.), *European Data Protection: Coming of Age*, New York, Springer; CAVOUKIAN, A. E CHANLIAU, M., *Privacy and Security by Design: A Convergence of Paradigms*, 2013, consultabile in http://www.privacybydesign.ca/index.php/paper/privacy-and-securityby-design-a-convergence-of-paradigms/.

dati personali) garantisce che siano trattati, di *default*, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In tal modo si garantisce che i dati personali non siano resi accessibili a un numero indefinito di persone e che gli interessati siano in grado di controllarne la distribuzione. Un ruolo fondamentale, in tutto ciò, spetta ai produttori, i quali hanno l'obbligo di attuare le misure e le procedure tecniche e operative adeguate per garantire che i loro servizi e prodotti consentano ai titolari del trattamento di conformarsi ai principi quivi esposti.

A conclusione di questa breve panoramica, è utile richiamare la voce di chi ha correttamente osservato che progettare sistemi informativi in un'ottica di "*privacy by design*" *"significa, infatti, primariamente, permettere all'utente, principale beneficiario delle misure considerate, di essere centro dei flussi di dati, appunto grazie alla definizione di strumenti* privacy-friendly"[61].

In ambito sanitario, di centrale interesse per il presente lavoro, l'adozione di una politica "*data protection by design and by default*" rappresenta la base per "*il* design *di nuove infrastrutture per la gestione della salute, consentendo di raggiungere un buon bilanciamento tra esigenze di cura individuale, tutela di diritti fondamentali del paziente e interessi di salute pubblica*"[62].

[61] R. BRIGHI; M.G. VIRONE, *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica*, in: *A Matter of Design: Making Society trough Science and Technology*, Milano, Open Access Digital Publication by STS Italia Publishing, 2014, p. 1218.

[62] R. BRIGHI; M.G. VIRONE, *cit.*: le autrici, auspicando che "*gruppi di esperti riflettano sulle nuove fattispecie, nate dalla sempre più diffusa applicazione delle Tecnologie dell'Informazione e della Comunicazione anche al settore sanitario*" compiono espresso riferimento, tra le altre, alla possibilità di raccogliere e trattare i dati sanitari in infrastrutture e servizi di "*cloud computing*" o nei dispositivi "*mobile*".

3. *Security and resilience in Governmental Clouds and in eHealth infrastructures & services*

All'inizio del 2011 l'ENISA (Agenzia Europea per la Sicurezza delle Reti e dell'Informazione) ha pubblicato i risultati di un'attività di studio denominata "*Security and Resilience in Governmental Clouds*"[63], alla quale hanno partecipato le principali multinazionali che erogano servizi di *cloud computing* insieme ai rappresentanti di governi, pubbliche amministrazioni e fornitori di servizi sanitari interessati ai servizi in *cloud*. Con lo studio si è cercato di comprendere se il mercato dei servizi in *cloud* fosse in grado di rispondere anche alle esigenze della P.A., in termini di *compliance* normativa, di sicurezza e di affidabilità. Lo scenario oggetto dello studio ENISA ha coinvolto un gruppo di ULSS/ASL italiane interessate ad adottare modelli di *cloud* per la gestione di servizi sia critici (come Fascicolo Sanitario Elettronico, referti e prenotazioni *on-line*) sia meno critici (come i servizi di *e-learning* per il personale).

I presupposti dai quali ha preso le mosse lo studio condotto dall'ENISA sono stati, da una parte, il forte impatto del settore sanitario nelle voci della spesa pubblica, con la conseguenza che la prima esigenza che si intende soddisfare con l'uso delle tecnologie *cloud* è proprio il risparmio economico, mantenendo elevato il livello di qualità dei servizi offerti. Dall'altra parte, però, vi è la consapevolezza dei rischi connessi a queste nuove modalità di gestione dei servizi, alla luce delle conseguenze dannose, anche in termini di reputazione, che potrebbero derivare da un eventuale malfunzionamento degli stessi. Per queste ragioni le amministrazioni sanitarie, prima di adottare le tecnologie *cloud* per l'offerta dei propri servizi, devono necessariamente analizzare l'impatto economico, tecnologico e normativo che questa scelta potrebbe comportare.

Muovendo da questi presupposti, il lavoro svolto dall'ENISA ha messo in evidenza come le soluzioni di *cloud computing* rappresentino valide alternative per l'offerta dei servizi sanitari, sia per i vantaggi economici sia per

[63] Il *report* è consultabile al seguente indirizzo: https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport

l'innovazione tecnologica che rappresentano. In tale contesto, però, la presenza di norme inadeguate e la percezione da parte di utenti e fornitori delle criticità legate alla *privacy* e alla tutela dei dati, costituiscono un grave ostacolo al passaggio verso tali modelli di offerta dei servizi[64].

L'analisi, svolta in un periodo precedente all'approvazione del Regolamento Privacy, si chiudeva con alcune raccomandazioni finali rivolte sia alle istituzioni europee che agli organi di governo dei Paesi membri UE, anche in virtù del piano di azione europeo in materia di sanità digitale elaborato dalla Commissione Europea[65], invocando la rimozione delle suddette barriere.

In particolare, per quanto attiene agli aspetti legati alla *privacy*, si riscontravano le seguenti necessità:

- armonizzare l'impianto normativo dei singoli Paesi membri, attraverso un intervento normativo da parte dell'Unione Europea[66];
- definire in modo chiaro e preciso i ruoli dei vari soggetti coinvolti nella filiera del trattamento dei dati sanitari (titolari e responsabili del trattamento), individuando con certezza gli obblighi e le responsabilità connesse ai vari ruoli;
- semplificare le norme poste a tutela dei dati personali e quelle in materia di sanità elettronica, al fine di garantire effettivamente i diritti dei pazienti;
- prevedere una regolamentazione coerente e omogenea in tutto il territorio europeo, affinché i vari fornitori *cloud* possano offrire servizi nel rispetto della *privacy* dei cittadini. In tal senso, secondo il principio della "*privacy by design*" (oggi introdotto con il RGDP) si auspicava che tutti i servizi e i prodotti dovessero essere realizzati sin dalla fase della loro progettazione in conformità con le regole *privacy*.

[64] L'inadeguatezza delle norme va valutata nell'intero contesto europeo, in cui il settore sanitario di ciascun Paese membro è regolato da normative spesso molto distanti e disomogenee, rendendo così difficile la nascita e il consolidamento di un vero e proprio mercato europeo dei servizi dell'*e-Health*.

[65] Il piano "eHealth Action Plan 2012-2020" è stato contenuto nella Comunicazione della Commissione Europea COM/2012/0736 final, consultabile all'indirizzo http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0736

[66] In questo senso, il già citato piano di azione europeo sull'eHealth 2012-2020 e il Regolamento (UE) 2016/679, rappresentano una valida risposta a queste esigenze.

Infine, per far fronte ai rischi e garantire la sicurezza nella sanità elettronica, secondo le raccomandazioni ENISA, ciascuno Stato doveva individuare e catalogare i rischi e gli aspetti critici delle proprie infrastrutture di *eHealth* ed elaborare delle linee guida per la protezione delle stesse.

3.1 Controllo e governo sui dati

Lo studio condotto dall'ENISA ha posto in evidenza come la riservatezza dei dati personali trattati con il *cloud computing* rappresenti una delle principali criticità di questa tecnologia.

A comprova dell'importanza di questa problematica, è stato opportunamente citato quanto affermato dal Presidente dell'Autorità Garante per la Protezione dei Dati Personali nella Relazione al Parlamento dell'anno 2009, secondo cui "*occorre riflettere anche sui rischi che pone la nuova tecnologia del* cloud computing*, con la quale i dati verranno sempre più sottratti alla disponibilità materiale di chi li produce e usa, e gestiti da enormi* server *collocati in ogni parte del pianeta. Un fenomeno che moltiplicherà i servizi di* remote hard disk *e renderà sempre più ampio il ricorso all'*outsourcing *e all'*hosting *dei sistemi, moltiplicando i servizi forniti da terzi secondo modalità che favoriscono sempre di più la delocalizzazione dei dati conservati*"[67].

Il ricorso alle tecnologie *cloud* comporta, quasi sempre, l'affidamento della gestione delle infrastrutture informatiche ad un soggetto esterno (*outsourcing*), coinvolgendo di fatto il *cloud provider* nel trattamento dei dati personali immessi nella nuvola che, il più delle volte, sono memorizzati nei *server* messi a disposizione e controllati dai vari fornitori dei servizi.

Tutto ciò assume un particolare significato dinnanzi all'aumento dell'uso delle tecnologie informatiche nella società moderna, in cui gran parte delle operazioni della vita quotidiana sono svolte con l'ausilio della tecnologia.

In questo contesto, le potenzialità offerte dal *cloud*, dalla consultazione in remoto da qualunque dispositivo all'incremento delle capacità di calcolo, hanno portato ad un aumento esponenziale delle informazioni e dei dati pro-

[67] La relazione è consultabile al seguente indirizzo: http://194.242.234.211/documents /10160/10704/1730115

dotti e, di conseguenza, una maggiore richiesta di spazi di memoria per le attività di ricerca dei suddetti e l'eventuale conservazione.
Questo approccio globale al fenomeno ha generato un aumento della domanda di servizi in *cloud* e, nel contempo, un abbassamento della consapevolezza degli utenti sui rischi legati, in particolar modo, ai dati immessi sulla "nuvola"[68].

Il concetto di controllo e governo dei dati è legato agli aspetti di interoperabilità e portabilità e quindi alla possibilità di migrare verso altri sistemi *cloud*, appartenenti ad altri *provider*. Si tratta di prerogative che ciascuna Amministrazione pubblica deve assicurarsi, attraverso un'attenta selezione del fornitore *cloud* per evitare il cosiddetto "*vendor lock-in*", ossia l'impossibilità di riversare i dati presso altri fornitori per ragioni di mancanza di interoperabilità tra i sistemi *cloud*. Solo in questo modo è possibile consentire la portabilità dei dati, un aspetto assai rilevante nel settore sanitario in cui il processo di cura e riabilitazione dei pazienti deve essere costantemente garantito ai massimi livelli su tutto il territorio nazionale e comunitario.

Non meno importante, nell'analisi condotta, è stato il profilo del controllo da parte di autorità (forze di polizia, governi)[69] o di altri soggetti terzi non autorizzati. Il complesso rapporto tra la riservatezza dei dati nel *cloud* e l'esigenza di sicurezza sia a livello nazionale che internazionale, come giustamente è stato osservato, è destinato sempre più a far discutere, da una parte, gli operatori del mercato, fornitori dei servizi in *cloud* e, dall'altra, le autorità governative e le forze di polizia.

[68] Il tema della riservatezza dei dati personali nell'ambito del *cloud computing* è già stato oggetto di approfondimento nei paragrafi precedenti.

[69] La criticità di questo aspetto è stata maggiormente compresa in una fase temporale successiva a quella in cui è stato condotto lo studio dell'ENISA, ossia in occasione del recenti casi che hanno interessato la cronaca internazionale e statunitense: il caso "*Safe Harbor*" (già trattato nel paragrafo 2.3), generato da un presunto potere di ingerenza sui dati della piattaforma *social* Facebook da parte delle autorità governative degi USA e il più recente caso della Apple che ha negato l'accesso all'FBI ai dati crittografati di un suo modello di *smartphone*, nell'ambito dell'indagine della polizia federale americana per la strage di San Bernardino.

3.2 La sicurezza

Nell'ambito di un altro studio[70], pubblicato nel 2015 sempre ad opera dell'ENISA, sono state esaminate le modalità di approccio e le misure di sicurezza adottate da ciascun stato membro dell'UE per garantire la sicurezza nella sanità.

Dall'indagine è emerso che per la maggior parte dei Paesi intervistati la sanità rappresenta un settore critico. I criteri di identificazione degli aspetti "delicati" della sanità elettronica sono i più vari: continuità operativa, sicurezza e integrità dei dati, disponibilità dei servizi, politiche di sicurezza e così via.

Non vi è dubbio che gli incidenti di *cyber*sicurezza, ovvero le violazioni delle misure poste a tutela della sicurezza dei sistemi, nell'ambito dell'*e-Health*, possano avere un enorme impatto e causare ingenti danni. Per queste ragioni è fondamentale che nell'ambito della sanità elettronica siano adottate misure che garantiscano allo stesso tempo la disponibilità dei dati, la continuità operativa e la resilenza, ovvero la capacità di mantenere un accettabile livello di servizio nonostante la presenza di fattori di disturbo dovuti al normale funzionamento del sistema. Con l'adozione di modelli basati sul *cloud computing*, queste caratteristiche devono, ancora di più, essere garantite da parte dei fornitori dei servizi e da parte delle singole amministrazioni sanitarie.

[70] "*Security and Resilience in eHealth*" (ENISA, 2015), consultabile all'indirizzo: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services

PARTE QUINTA - I CONTRATTI DEL *CLOUD COMPUTING*

1. Il rapporto tra il contratto di *cloud computing* e la "categoria" dei contratti informatici

L'inesistenza di norme positive dedicate ai contratti di *cloud computing* impone, come di regola accade ogni volta che si approccia la materia dei contratti legati alle tecnologie informatiche e telematiche, il ricorso, laddove possibile, alle norme già vigenti nell'ordinamento italiano, anche se non dettate con specifica attenzione per questa tecnologia (o meglio, tenuto conto delle molteplici varianti del *cloud computing*, per queste fattispecie).

Alla base del *cloud computing*, come si è avuto modo di illustrare nelle prime due parti del presente lavoro, non c'è nulla di completamente nuovo, in quanto la sua logica è la medesima dei servizi *on-line*, tradizionalmente erogati ai consumatori finali (tramite *e-mail* e *social networks*) ma con la peculiarità di rivolgersi al mondo del *business* e della Pubblica Amministrazione attraverso la sostituzione di *hardware* e *software* con collegamenti *on-line* verso centri (banche dati) remoti. In sintesi, il *cloud computing* è un nuovo modo di fornire risorse, non una nuova tecnologia.

Ci si trova, pertanto, dinnanzi ad un contesto che, considerato nei singoli frammenti che lo compongo, non è nuovo per il mondo dei giuristi, che si sono occupati diffusamente di contratti informatici[1] in senso lato e in senso

[1] Tra le autorevoli voci che si sono occupate dei contratti informatici, si vedano, per tutti: IASELLI M., *I contratti informatici (III edizione)*, Altalex 2015; ALPA G., *I contratti di utilizzazione del* computer, in Giur. it 1983, IV, 42 ss.; ARNÒ G., *I contratti relativi all'*hardware, in I contratti, 1995, 224 ss.; BRAGGION A., *La validità delle clausole che limitano od escludono la responsabilità nei contratti per la fornitura di* software*: una rassegna di recenti pronunzie nella giurisprudenza europea*, Riv. dir. ind. 1989, I, 217; BRAVO F., *Appalti pubblici per la fornitura di beni e servizi nel settore ICT e tecniche di redazione contrattuale. Le linee guida del CNIPA*, in Dir. inf. e informatica, 2007, 103 ss.; CERINA P., *Contratti internazionali di informatica e Legge applicabile, prime considerazioni, in Dir. Infor e informatica*, 1994, 405 ss; D'ARRIGO, *Prospettive della c.d. licenza a strappo nel nostro ordinamento*, in Dir. Inf., 1996, 462-468; FALLETTI G., *Il contratto di* application service providing, in Il Dir .infor e informatica, 2001, 411 ss.; MAGGI M., *Il contratto di fornitura di sistema informatico come contratto indeterminato*, nota a Cass. Sez. II, 22 marzo 1999, n. 2661,

più ristretto. Nell'accezione più ampia sono compresi tutti i contratti che fondano la loro funzione economico-sociale sull'informatica, i contratti di utilizzazione degli strumenti dell'informatica, i contratti di acquisizione, elaborazione e diffusione di dati a mezzo di strumenti informatici, nonché i contratti che si formano attraverso gli strumenti dell'informatica ed ogni altra attività giuridicamente rilevante che possa essere compiuta adoperando l'elaboratore come mezzo di formulazione dell'atto o di trasmissione dell'atto. In senso stretto, invece, sono annoverabili nella categoria dei contratti informatici, quelli cibernetici[2] e quelli telematici[3].

In questa quinta parte, dedicata ai contratti di *cloud computing*, non si può prescindere da un breve *excursus* sul contratto informatico, le cui caratteristiche si ripresentano anche per i negozi quivi trattati.

---

in I Contratti, 1999, 995 ss.; MUSELLA A., *Il contratto di outsourcing del sistema informativo*, in Dir. Infor. E informatica, 1998, 857 ss.; PIANA C., *Licenze pubbliche di* software *e contratto*, in I Contratti, 2006, p. 720; RICOLFI M., *I contratti dell'informatica*, reperito all'URL: www.jus.unitn.it/cardozo/review/Contract/Ricolfi-1998/sena1.htm; ROSSELLO C., *La responsabilità da inadeguato funzionamento di programmi per elaboratori elettronici. Aspetti e problemi dell'esperienza nord americana*, in Riv. crit. dir. priv., 1984; ROVERSI R., *I contratti di* outsourcing *della manutenzione*, in I Contratti, 1997, pagg.522 ss.; SAMMARCO P., *Appalto di* software *e trasferimento di diritti*, in Giustizia civile, 1998, 97 ss.; SAMMARTANO F., *I contratti informatici*, reperito all'URL: www.diritto.it/articoli/civile/sammartano.html; SCUFFI M., I *Contratti per la manutenzione: verso il "*global service*"*, in Il Diritto Industriale, 1996, 344 ss.; TOSI E., *Brevi note a margine del problema della qualificazione e dell'inadempimento del contratto di fornitura di* hardware *e* software, nota a Tribunale di Bari, 4 giugno 1994, in Il Dir. infor. e informatica, 1995, 933 ss.; TOSI E., *Natura e qualificazione dei contratti di fornitura dei sistemi informatici*, nota a Tribunale Torino, 13 marzo 1993, in Dir. Infor. e informatica, 1995, 386 ss.; ZACCARIA A., *La responsabilità del produttore di* software, in Contratto e impresa, 1993, 294 ss.

[2] Vengono conclusi automaticamente e, cioè, tra una persona e un *computer* ovvero tra *computers* come parti contraenti contrapposte. Nella seconda ipotesi, successivamente alla programmazione dell'elaboratore, la formazione della volontà contrattuale è opera del *computer* senza alcun intervento umano.

[3] La loro peculiarità è costituita dal fatto che le volontà dei contraenti (proposta e accettazione), vengono trasmesse per via telematica. Si tratta di fattispecie perfettamente riconducibili al disposto dell'art. 1321 c.c., come tutti i negozi conclusi a distanza (per es. per mezzo del telefono).

1.1 I confini comuni

Il primo aspetto da considerare è proprio collegato alla difficoltà di definire un'unica categoria di contratti informatici. Si tratta, infatti, più precisamente, di molteplici fattispecie negoziali connesse a beni e servizi rientranti nel comparto dell'informatica per le quali, al di là di questo debole denominatore, non è individuabile una *ratio* comune.

L'incertezza nell'inquadramento giuridico dei contratti informatici ha risvolti notevoli anche relativamente ai contratti di *cloud*, per i quali "*diviene arduo individuare le giuste tecniche per garantire la sicurezza dell'elaborazione, conservazione, estrazione, condivisione, circolazione dell'informazione dotata di valore giuridico (come gli atti di un'amministrazione sanitaria). Diviene altrettanto arduo comprendere e normare la gestione dei flussi informativi, l'elaborazione e comunicazione della conoscenza internamente alle strutture sanitarie e tra queste e il cittadino/paziente*"[4].

Nonostante la dichiarata disomogeneità dei contratti informatici, spesso capita di imbattersi in fattispecie dai connotati comuni, tra i quali, il primo da ricordare, tipico anche dei negozi di *cloud*, è il notevole squilibrio di forza contrattuale che sussiste tra fornitore e cliente[5]. Ne consegue che i contratti informatici non sono frutto di un accordo fra le parti, quanto piuttosto mezzo attraverso il quale il soggetto più forte vincola il soggetto più debole, con la conseguenza che risulta indispensabile in ogni ordinamento apprestare strumenti che consentano un controllo sostanziale ed un maggior equilibrio degli interessi contrapposti.

Nella prassi commerciale i contratti di *cloud computing* sono predisposti unilateralmente dai *cloud providers*, i quali non sempre forniscono tutte le informazioni necessarie in merito alla collocazione dei *server* o alle misure di sicurezza adottate e non esplicitano chiaramente le garanzie offerte al fruitore dei servizi da loro erogati, riservandosi ampi poteri e prevedendo clausole di esclusione della propria responsabilità. Sebbene la scarsa trasparenza e la carenza di garanzie tipica di questi contratti può non rappresentare

[4] MANCARELLA M., *cit.* p. 216.;

[5] Sul ruolo delle parti si è già avuto modo di trattare nella parte quarta al paragrafo 2.4 "Difficoltà di inquadramento soggettivo".

un aspetto rilevante per un utente che utilizza il *cloud* per scopi personali, dinnanzi ad un contratto che vede coinvolti enti pubblici, imprese o professionisti, che sono tenuti ad osservare precisi obblighi di legge, questi aspetti non possono essere tollerati. La Pubblica Amministrazione, ad esempio, deve sottostare alla disciplina dei contratti pubblici e potrebbe, a causa di un contenuto negoziale imposto *cloud provider*, non garantire la necessaria coerenza alle suddette disposizioni[6].

Tutti i fruitori di servizi in *cloud* devono, quindi, essere consapevoli dei rischi e delle vulnerabilità della tecnologia che utilizzano anche e soprattutto sotto il profilo delle implicazioni giuridiche.

Da questo punto di vista, può affermarsi la riconducibilità ai cosiddetti contratti per adesione, ove la fase delle trattative contrattuali è inesistenze con la conseguenza che non si definiscono alcuni aspetti assai delicati (responsabilità, i livelli di servizio, la legge applicabile e altri ancora) già sopra citati.

Il disequilibrio tra le parti, non è sempre basato sulla forza economica dei contraenti. La grande diffusione del *cloud computing*, infatti, coinvolge spesso, quali fruitori del servizio, soggetti tutt'altro che deboli, come ad esempio le Pubbliche Amministrazioni (anche di notevoli dimensioni). La disparità, sempre più spesso, inerisce alla cultura informatica delle parti e ciò incide inevitabilmente sull'equilibrio contrattuale. Nell'ordinamento italiano, un correttivo a tale problema è rappresentato dagli obblighi di corretta informazione, che sussistono sia nella fase precontrattuale, in base al disposto dell'art. 1337 c.c., sia nella fase di esecuzione del contratto in base al ge-

[6] AgID, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, cit. p. 19. Con specifico riferimento alla materia dei contratti pubblici, va specificato che le Raccomandazioni sopraccitate sono state pubblicate sotto la vigenza del D.lgs. 12 aprile 2006, n. 163 e del Regolamento attuativo DPR n. 207/2010, che di recente sono stati espressamente abrogati dall'articolo 217, comma 1, del Decreto legislativo 18 aprile 2016, n. 50 "*Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e fornitu*re". Pertanto, auspicando il pronto rilascio di una nuova versione (quella attualmente pubblicata è la 2.0), la lettura odierna delle Raccomandazioni di AgID, va eseguita tenendo conto delle intervenute modifiche normative, con la possibilità di sostituzione automatica per le sole parti compatibili.

nerale dovere di correttezza e di buona fede di cui all'art. 1375 c.c.. La violazione di tali obblighi determina, nel primo caso, una responsabilità precontrattuale che può determinare anche l'annullabilità del contratto, qualora sia configurabile il vizio del dolo per reticenza, ovvero l'errore essenziale sull'oggetto del contratto; nel secondo caso, invece, dà luogo al risarcimento del danno, ovvero alla risoluzione del rapporto.

L'informatizzazione, in passato, dal punto di vista negoziale, comportava sempre contemporaneamente l'acquisto o il noleggio (anche nella forma del *leasing*) di tutto l'*hardware* e il *software* necessario. Ciò si traduceva, in alcuni casi, nella necessità di dover stipulare un unico contratto con un unico fornitore, in altri casi più complessi, più contratti con diversi fornitori. Nell'ambito del *cloud computing*, dominato dai concetti di virtualizzazione e remotizzazione, si stipulano prevalentemente contratti aventi ad oggetto il *software* (la licenza d'uso, il contratto di sviluppo del *software* e il contratto di assistenza e manutenzione) e i servizi informatici (appalto, *outsourcing*, integrazione sistemi, *disaster recovery*, *engineering*).

In effetti, però, anche per gli acquisti effettuati da un unico fornitore (che si tratti di informatizzazione in senso "storico" ovvero di migrazione sul *cloud*) può parlarsi di contratti separati, e ciò vale tanto per acquisti eterogenei (*hardware*, *software* e relativi servizi) così come per gli acquisti omogenei (soltanto *hardware* o soltanto *software* e relativi servizi).

A fronte delle problematiche che potrebbero sorgere dall'eccessivo "frazionamento" dei rapporti contrattuali, sono possibili due soluzioni:

a) dar vita ad un "collegamento negoziale" tra i contratti (che altrimenti rischierebbero di rimanere nell'ambito dei meri "motivi"), vincolando la stipula di detti contratti alla realizzazione dello scopo comune prefissato e prevedendo che il mancato adempimento di uno di loro determini la possibilità di porre nel nulla anche gli altri;

b) stipulare un unico contratto "misto" (tale si definisce un contratto che incorpora rapporti riconducibili a "tipi" legali diversi) avente ad oggetto la realizzazione dell'obiettivo complessivo delle parti.

Il risultato del riconoscimento dell'unitarietà del rapporto potrà avere senz'altro conseguenze rilevanti, non solo in caso di inadempimento di un contratto, ma anche in caso di nullità o nel caso di impossibilità sopravvenu-

ta di una delle prestazioni, in quanto in tali casi l'intero unico negozio verrebbe travolto.

Nel caso del collegamento negoziale, invece, ciascuno dei contratti conserverà la propria specifica disciplina. In tal caso, però, atteso che comunque occorre rifarsi alla disciplina tipica propria dei contatti richiamabili, occorre chiarire quale sarà applicabile al contratto "misto". La dottrina[7], a tal proposito, suggerisce l'adozione di due distinti criteri:

a) il criterio dell'assorbimento[8] (o della prevalenza), che prevede che ai contratti misti vada applicata la disciplina del contratto ritenuto "prevalente";

b) il criterio della combinazione, ai sensi del quale la disciplina del contratto misto viene ricostruita attraverso l'applicazione, in quanto compatibili, delle discipline specifiche applicabili a ciascun elemento che compone contratto misto.

Entrambi gli approcci presentano dei limiti, in quanto, mentre il principio della combinazione tende inevitabilmente a frammentare il dettato contrattuale, finendo per sacrificare l'unitarietà del rapporto, dall'altro il principio dell'assorbimento finisce per sacrificare le specificità dei singoli tipi contrattuali che compongono il contratto misto.

2. Tentativi di inquadramento

Fatte le premesse di cui ai precedenti paragrafi, per inquadrare meglio il contratto di *cloud computing* e, quindi, individuarne la disciplina positiva applicabile è bene ripartire dall'analisi della relazione negoziale tra le parti del contratto[9].

[7] Cfr. per tutti CARINGELLA F., BUFFONI L., Manuale di diritto civile - V Edizione, 2015, p. 21.

[8] Nell'applicazione pratica è il di regola seguito dalla giurisprudenza. Si vedano, tra le tante, Cassazione Civile, sez. II, sentenza 12/12/2012 n° 22828; Cassazione Civile, sez. II, sentenza 22/03/1999, n. 2661; Tribunale di Torino, 13/03/1993.

[9] Cfr. BELISARIO E., *"Cloud Computing", Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 11 e ss.

Nella prima parte del presente lavoro[10] si è già avuto modo di specificare che il *cloud computing* si sostanzia nell'erogazione di servizi, tanto che nelle classificazioni convenzionalmente adottate si utilizzano le locuzioni: *"Software as a Service"," Platform as a Service"* e *"Infrastructure as a Service"*[11]. Questa connotazione assume rilevanza anche dal punto di vista giuridico, in quanto la gestione delle risorse informatiche, sia in ambito pubblico che privato, non è più una prerogativa esclusiva del fruitore del servizio (che era anche proprietario delle strutture *IT*). Con l'avvento del *cloud* e dei servizi erogati attraverso questo nuovo paradigma, le risorse informatiche sono spesso[12] di proprietà del terzo fornitore del servizio il quale consente al fruitore l'accesso diretto ad esse. L'informatica, quindi, esce dall'azienda e rientra sotto forma di possibilità di accesso ad essa[13]. Con questo meccanismo il fruitore perde il tipico controllo e la gestione diretta che, prima del *cloud*, poteva esercitare in qualità di proprietario delle infrastrutture informatiche. Questo mutamento di prospettiva è testimoniato sia dalla letteratura giuridico economica sia in quella sociologica, quando si discute di "cultura dell'accesso"[14], secondo cui non assume più rilevanza la qualifica di proprietario delle risorse bensì la possibilità di poter accedere alle stesse secondo condizioni stabilite dai soggetti terzi che le detengono ed erogano i servizi.

La nuova visione del rapporto assume notevole rilevanza anche dal punto di vista negoziale; infatti, data la centralità dei servizi offerti, sarà fondamentale determinare correttamente ed attentamente il contenuto degli accor-

---

[10] Si veda anche quanto contenuto nelle "*Raccomandazioni e proposte sull'utilizzo del* cloud computing *nella Pubblica Amministrazione*" e nelle Linee guida *"caratterizzazione dei sistemi cloud per la Pubblica Amministrazione*" pubblicate da Agid, di cui si è trattato nella parte terza.

[11] Cfr. MANCARELLA M., "E-health *e diritti, l'apporto dell'informatica giuridica, 2012, p. 215*.; MANTELERO A., *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. Informaz.informat., 2010, pp.682 e ss.

[12] Fanno eccezione, come si dirà nel prosieguo, i servizi di *hosting* e di *housing*, rientranti nella tipologia "*Infrastructure as a Service*" (IaaS).

[13] La teoria dell'informatica come servizio, anziché come bene, è risalente nel tempo, cfr. D.F. PARKHILL, *The Challenge of the Computer Utility*, Reading (Mass.), 1966.

[14] RIFKIN J., *L'era dell'accesso*, Milano, 2000 e, con specifico riferimento ai servizi di cloud computing, SUN MICROSYSTEMS, *Introduction to the Cloud Computing Architecture, White Paper*, 1st Edition, giugno 2009, in *http://webobjects.cdw.com* ed INTERNATIONAL TELECOMUNICATION UNION, *Distributed Computing: Utilities, Grid & Clouds*, 2009, in *www.itu.int*.

di contrattuali che disciplineranno il servizio, i quali dovranno prevedere la continuità della prestazione e la cooperazione tra fornitore e utilizzatore.[15]

Permane anche nell'informatizzazione di nuova generazione, la presenza contemporanea di più negozi riconducibili ad un'unica operazione di approvvigionamento e da qui risorgono, seppur con veste differente, i tentativi di riconduzione dei contratti di *cloud computing* alle categorie dei contratti tipici (prevalentemente appalto di servizi o contratto d'opera) ovvero a quella dei contrati atipici (per es. licenza d'uso, *outsourcing*, *hosting*, *housing*, *Disaster recovery*, ecc.), con doverosa attenzione ai contratti misti.

2.1 Tra l'appalto di servizi e la licenza d'uso

Un primo orientamento[16] osserva come i contratti di *cloud* siano dotati di una struttura composta contemporaneamente da elementi caratteristici del contratto di appalto di servizi e di licenza d'uso.

Così, come nell'appalto di servizi l'obbligazione assunta dall'appaltatore consiste in un *facere*, ovvero nella fornitura di un servizio verso un corrispettivo in denaro, pattuito con il committente, così, nei contratti di *cloud computing*, l'obbligo che assume il fornitore del servizio consiste nella messa a disposizione di spazio di memoria, risorse computazionali ed altri servizi. Da questo primo confronto si rileva che l'obbligazione assunta dal *cloud provider* (al pari di quella assunta dall'appaltatore) è da considerarsi di risultato, essendo il fruitore soddisfatto solamente con l'esatta fornitura dei servizi pattuiti in contratto.

---

[15] Tra i tanti, MANTELERO A., *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. Informaz.informat., 2010.

[16] In questo senso MANTELERO A. nella relazione: *"Il cloud computing, inquadramenti giuridici e differenze di approccio contrattuale"* tenuta dall'autore al convegno di Milano del 17 gennaio 2012 :"*Cloud Computing - I diversi approcci contrattuali e nuove definizioni in ambito privacy"*. L'audio di tale intervento e la relativa presentazione sono fruibili *on-line*. Sulle diverse tesi in ordine alla natura del contratto di *cloud* cfr.: BENDANI S., Software as a Service *(Saas): aspetti giuridici e negoziali*, in http://www.altalex.com/index.php?idnot=44076; FABIANO N., *I nuovi paradigmi della rete.* Distribueted computing, cloud computing e "computing paradigms":abstract *sugli aspetti e profili giuridici*, in http://www.diritto.it/art.php?file=/ archivio/27973.html

Il contratto di licenza d'uso consiste, invece, in un accordo attraverso il quale il licenziante consente l'utilizzo di un prodotto, solitamente un programma informatico, al licenziatario stabilendo modalità e obblighi a cui l'utente deve conformarsi nell'uso del prodotto stesso. Nella fattispecie dei contratti del *cloud*, lo schema della licenza d'uso si sostanzia nell'attribuzione del diritto di utilizzo di un *software* da parte dei fruitori.

Ebbene, nella prassi commerciale, i *cloud provider* propongono diverse soluzioni contrattuali che presentano, in combinazione, talvolta gli elementi predominanti dell'appalto di servizi e talaltra quelli tipici della licenza d'uso. È proprio osservando tali fattispecie, che la dottrina sopraccitata ritiene atipici (o meglio misti[17]) tali negozi, non essendo possibile ricondurli esclusivamente ad un tipo.

Concentrando l'analisi sui servizi informatici, è agevole notare che essi sono riferibili a tutti quei contratti che hanno ad oggetto un'attività riguardante un sistema informatizzato: dai contratti di assistenza o manutenzione di sistemi informatici, da una parte, a quelli che hanno ad oggetto una prestazione di attività automatizzate, dall'altra. Nonostante il denominatore comune, sono presenti differenze che, per ragionare sulla qualificazione giuridica, e quindi sulla disciplina applicabile a ciascuna delle categorie suddette, è necessario procedere distintamente. I primi, ossia i contratti che hanno per oggetto una normale prestazione, consistente nello svolgimento di un'attività materiale o intellettuale di tipo tradizionale, la cui unica peculiarità è l'oggetto della condotta (connesso ad un sistema computerizzato), non comportano particolari problematiche di inquadramento. Al contrario, la natura particolare della prestazione automatizzata richiede un esame più approfondito delle regole della disciplina codicistica, proprio per il prevalere di aspetti del tutto peculiari, i quali rendono difficile il ricorso a categorie tradizionali di riferimento.

Per le prime fattispecie è possibile richiamare le disposizioni del codice civile che distinguono nettamente tra prestazione d'opera e prestazione di un servizio dettando differenti discipline. Nel caso di prestazione informatizzata, invece, non è sempre chiaro se la stessa possa assimilarsi ad un'opera ovvero ad un servizio e, proprio sotto questo profilo, appare preferibile sostenere l'applicabilità di una disciplina mista e cioè, come già detto, di norme

[17] Sui contratti misti, si veda quanto illustrato al paragrafo precedente.

in parte di un istituto e in parte di un altro. Potrebbe così trattarsi di contratto di appalto, così come di contratto d'opera, i quali si distinguono soltanto sotto il profilo della responsabilità dell'organizzazione dei mezzi. Entrambi, quindi, possono avere ad oggetto la realizzazione di un'opera, intesa come risultato dell'attività creativa del debitore, ovvero in un servizio[18] prestato in maniera continuativa che pur non comportando un incremento patrimoniale in senso stretto del committente ne realizza l'interesse negoziale.

Altri autori[19], con particolare riferimento ai servizi di *cloud* SaaS hanno ritenuto che "*la prevalenza di una prestazione di fare, avente ad oggetto la fornitura di uno o più servizi* software *o di altra natura, unitamente alla presenza di un'organizzazione dotata di mezzi e gestione propri e al pagamento di un corrispettivo sono tutti elementi che fanno propendere per la configurabilità di un appalto di servizi sia pure avente ad oggetto prestazioni continuative o periodiche. La prima diretta conseguenza di tale inquadramento è che l'obbligazione dell'appaltatore costituisce un'obbligazione di risultato, anche se nella pratica non mancano casi di soggetti interessati a far figurare nel contratto i propri obblighi come mezzi*".

Per quanto concerne la componente dei contratti di *cloud* riconducibile alla licenza d'uso di un programma per elaboratore, questa sarà presente in tutti i casi in cui nel servizio offerto dal fornitore sia compreso, dietro corrispettivo, il diritto di utilizzare in modo non esclusivo uno o più *software*, spesso residenti nei server remoti del *cloud provider*.

---

[18] "*Nell'appalto di servizi […] il contenuto della obbligazione è una prestazione di fare, che ha ad oggetto il compimento di un servizio, il quale dà luogo solo ad una produzione di utilità (e non ad una trasformazione di materia) […]. In altri termini, mentre nell'appalto d'opera l'*opus*, realizzatosi attraverso la trasformazione della materia, unifica in sé l'attività e la materia, per cui la detenzione dell'opus da parte dell'appaltatore è sempre anche nel suo interesse (incorporandosi in essa l'attività); nell'appalto di servizi, invece, operandosi la produzione di utilità distinte dalla res (che resta un mero strumento attraverso il quale il servizio si svolge), l'interesse dell'appaltatore si rivolge alla produzione delle utilità, con la conseguenza che la detenzione della res da parte sua (restando la res distinta dall'attività) viene posta in essere nell'interesse del committente*": Cass. civ. Sez. II, 17.4.2001, n. 5609.

[19] BENDANDI S., Software as a service (SaaS). *Aspetti giuridici e negoziali*, in Altalex, 18 dicembre 2008, http://www.altalex.com/documents/news/2008/12/18/software-as-a-service-saas-aspetti-giuridici-e-negoziali; Nello stesso senso BELISARIO E., "Cloud Computing", Informatica Giuridica – collana diretta da Michele Iaselli - eBook n.17, Altalex 2011, pag. 12 e ss.

L'inquadramento giuridico delle licenze d'uso, che si presentano, già per il loro *nomen iuris*, come negozi atipici, necessita di una approfondita indagine sulla volontà delle parti per, poi, ricondurre il regolamento concretamente adottato all'interno di uno specifico tipo codicistico (normalmente vendita o locazione), ovvero collocarlo quale espressione della libertà contrattuale sancita all'art. 1322 c.c.

Il termine licenza d'uso, dal punto di vista prettamente civilistico è sconosciuto all'ordinamento italiano e, di conseguenza, non ha una valenza tecnico-giuridica in sé insita. Soltanto il termine uso, inteso come diritto d'uso, è familiare al diritto privato. La licenza, invece, è tipica del diritto amministrativo ed ha una valenza autorizzativa.

Fatta questa precisazione, è possibile affermare che lo schema contrattuale della vendita potrebbe, probabilmente, essere invocato nelle distribuzioni che non prevedono alcuna riserva di diritti esclusivi per l'autore. Infatti, l'immissione dell'opera nel mercato, attraverso un contratto riconducibile alla previsione dell'art. 1470 c.c., non conserva il privilegio dei diritti esclusivi di controllo in capo al venditore ma, al contrario, esaurisce tutti i diritti patrimoniali di quest'ultimo sul bene alienato.

D'altronde, non potrebbe essere altrimenti, se si tiene in dovuta considerazione il cosiddetto principio dell'esaurimento, per il quale "*la prima vendita di una copia del programma nella Comunità Economica Europea da parte del titolare dei diritti, o con il suo consenso, esaurisce il diritto di distribuzione di detta copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso*"[20]. Si tratta di un principio di ordine pubblico, inderogabile dalle parti, già previsto per le altre opere dell'ingegno. L'unica condizione imposta dalla legge affinché si producano gli effetti del principio di esaurimento è la precisa scelta delle parti di uno schema negoziale perfettamente coincidente, in quanto dotato di tutti gli elementi essenziali, con il contratto di vendita. Diviene, pertanto, di fondamentale importanza capire, al di la della denominazione utilizzata, a quale modello negoziale tipico abbiano voluto aderire le parti.

Nelle altre ipotesi, invece, nelle quali l'autore non esaurisce i suoi diritti esclusivi e continua a governare la distribuzione dell'opera, le variabili da

[20] Art. 64 *bis*, lett. c), L. 633/1941.

considerare sono molteplici ed anche in questo caso non mancano i tentavi di riconduzione alle fattispecie codificate; prima fra tutte la locazione. In particolare, a partire dagli anni '80 si sono intervallati molteplici tentativi di inquadramento, le cui Voci[21] dominanti hanno evidenziato la corrispondenza tra il modello contrattuale delle licenze d'uso e quello della locazione, basandosi esclusivamente sull'oggetto della cessione, ossia il diritto di godimento sul software.

Risultava, per tale orientamento, fuorviante l'attribuzione del nome licenza ad una figura giuridica che si presenta sostanzialmente come locazione: "*diciamo locazione e non diciamo invece licenza, poiché la figura della licenza evoca altre cose*"[22].

In effetti, il contratto di locazione, previsto agli artt. 1571 ss. c.c., presenta delle caratteristiche non perfettamente coincidenti con ciò che, in pratica, rientra sotto il nome licenza d'uso. La locazione è un contratto consensuale il cui effetto principale è quello di costituire, in capo al conduttore, un diritto personale di godimento sulla cosa locata e, in capo al locatore, l'obbligo di far godere la cosa stessa al conduttore. Le principali obbligazioni del locatore sono: consegnare cosa locata in buono stato di manutenzione; mantenere la cosa in stato da servire all'uso convenuto; garantire al conduttore, durante la locazione, il pacifico godimento della cosa. Il conduttore è, da parte sua, obbligato a osservare la diligenza media nel servirsi della cosa per l'uso pattuito o per quell'uso che, secondo le circostanze, può presumersi; restituire la cosa al termine della locazione nel medesimo stato in cui l'ha ricevuta; dare il corrispettivo nei termini convenuti. Ebbene, com'è vero che il comune denominatore, tra il contratto di locazione e quello di licenza d'uso, è senz'altro la cessione del diritto di godimento sul programma dietro corrispettivo pecuniario, è altrettanto certo che tutti gli altri effetti tipici della locazione, sopra richiamati, sono estranei alle principali distribuzioni di *software* pacchettizzato.

---

[21] GALGANO F., *La cultura giuridica italiana di fronte ai problemi informatici*, in G. Alpa, V. Zeno Zencovich, I contratti d'informatica, 1986, p. 379; LEONE S., *La concessione del software tra licenza e locazione*, in G. Alpa, V. Zeno Zencovich, I contratti d'informatica, 1986, p. 349 ss.; FINOCCHIARO G., *I contratti ad oggetto informatico*, 1993, p. 94 ss; TOSI E., *I contratti di informatica*, Il Sole 24 Ore, 1993, p. 157 ss.

[22] GALGANO F., *cit*. p. 380

In numerosi casi il programma viene ceduto senza l'apposizione di un termine finale del diritto di godimento e, di conseguenza senza la possibilità, per il licenziante, di rientrarne in possesso; infine, senza espressa previsione del divieto di ulteriore cessione.

Il licenziante ha, certamente, l'obbligo di consegnare il bene esente da vizi ma, dal canto suo, il licenziatario non ha l'obbligo di restituire il programma alla scadenza (se prevista) della licenza. Il licenziatario, inoltre, non risponde nei confronti del licenziante in caso di perdita o deterioramento del bene; egli sopporta il rischio in prima persona come se fosse il proprietario del bene. Tutto ciò è più che sufficiente per escludere l'esatta coincidenza tra il contratto di locazione e la licenza d'uso, in favore di una locazione atipica[23].

Tuttavia, questi non sono gli unici modelli di riferimento per i contratti del *cloud*.

2.2 I contratti *Software as a Service*.

Nei servizi *cloud* di tipo SaaS "*il cliente affida al fornitore la gestione di alcune attività oppure fruisce direttamente, a mezzo di connessione remota, di programmi presenti sui* server *dello stesso, accedendo ad essi attraverso terminali finalizzati alla mera visualizzazione e inserimento (ossia senza alcuna capacità elaborativa)*[24].

Ancor prima della diffusione del *cloud computing*, tali servizi erano noti alla dottrina come *Application Service Providing* (*ASP*), che si concretizzavano, ad esempio, come: la gestione del servizio di elaborazione di paghe e contributi o della contabilità di un magazzino (*Enterprice Resource Planning* o *ERP*), il servizio di posta elettronica, il servizio di gestione completa del flusso documentale (*Document Management* o *DM*), il servizio di gestione delle trattative *on-line* (cosiddetto *e-procurement*) ed, infine, il servizio di gestione dei contatti con la clientela (cosiddetto *Customer Relationship Management* o *CRM*). Oggi, anche alla luce della presente ricerca, ai

[23] ROSSELLO C., *I contratti dell'informatica nella nuova disciplina del* software, 1997, p. 66; BONAZZI E., TRIBERTI C., *Guida ai contratti dell'informatica*, 1990, p. 57

[24] ABETI R., *I nuovi contratti: nella prassi civile e commerciale*, 2004, p. 127.

suddetti servizi può certamente essere aggiunta la gestione dei servizi sanitari, meglio nota come *e-health*.

In questo tipo di contratti, generalmente il fornitore provvede a tutte le operazioni necessarie al corretto funzionamento del prodotto: correzione di errori, sostituzione del programma o parti di esso con le versioni più aggiornate, personalizzazioni, ecc. In effetti, la prestazione offerta dal produttore è, soprattutto, di servizio e, in minor parte, di concessione in godimento del prodotto.

Potrebbe certamente osservarsi, a tal proposito, che l'utilizzatore gode del diritto di utilizzazione del *software*, come avviene per le classiche licenze è che l'unica differenza è la fruizione mediata, su piattaforma remota.

Aspetto questo che, notevolmente, allontana la posizione del licenziatario classico dal licenziatario ASP, se non altro per la preclusione che quest'ultimo patisce su tutti i diritti di utilizzazione che, di legge, gli spettano; si pensi, tra tutti, alla facoltà di decompilazione (nei limiti previsti dal legislatore), ovvero alla possibilità di realizzare la copia di riserva.

L'utilizzatore, non è in possesso di un'esemplare del programma e non ne ha una copia da installare sul proprio *pc*; è, pertanto, un'ovvia conseguenza che esso sia limitato in tutte le principali facoltà. Perciò, se di norma il licenziatario acquista il diritto di riprodurre l'opera, nel contratto di *cloud* SaaS questo diritto si azzera in quanto il prodotto è integralmente gestito dal fornitore.

Si consideri però, che i contratti in esame si presentano, spesso, con una variante, e cioè la parziale installazione del programma, anche in misura stabile, sull'elaborare dell'utilizzatore. Ecco che in questi particolari casi, la fattispecie è ancora diversa e presenta alcuni connotati delle licenze tradizionali (di cui si è detto al paragrafo precedente), con parziale riespansione delle facoltà del licenziante.

In generale, e salvo situazioni ibride, i contratti di *cloud* SaaS, come si è già avuto modo di illustrare nel precedente paragrafo, è, a tutti gli effetti, un appalto di servizi, in quanto diretto a produrre un'utilità al cliente, ovvero a soddisfare un suo interesse specifico[25]. Si rinvia, pertanto, a quanto già trattato in precedenza.

[25] BELISARIO E., cit. p. 12 e ss. Nel medesimo senso si è espressa anche l'AgID con le già citate "*Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministra-*

A tale orientamento si potrebbe obiettare che i servizi erogati tramite i contratti suddetti non vengono realizzati "*di volta in volta per i singoli utenti, ma questi ultimi si limitano a utilizzare servizi già precedentemente realizzati. La circostanza ora detta non consentirebbe di far rientrare il contratto cloud tra quelli di appalto di servizi*"[26] bensì nel novero dei contratti atipici.

Sul versante dell'atipicità può altresì aggiungersi che il contratto di *cloud* SaaS:

- è totalmente svincolato dall'ubicazione fisica del fruitore del servizio, il quale può collegarsi, ai *servers* del *provider*, da qualunque postazione remota;
- assicura servizi che possono essere utilizzati sulla base dell'esigenza dell'utente (quindi è caratterizzato da flessibilità e scalabilità);
- ha un costo variabile sulla base dell'effettiva intensità di utilizzo.

2.3 La "locazione" di spazio *web*

Mediante i contratti di *cloud computing* si erogano anche i servizi IaaS (*Infrastructure as a Service*) di *hosting* e *housing* noti anche come locazioni di spazio *web*.

In particolare, con il contratto di *hosting* "*[…] il prestatore di servizi concede l'utilizzazione di uno spazio all'interno del proprio disco rigido alle condizioni e secondo le modalità previste dal contratto […]*"[27].

La messa a disposizione di uno spazio (seppur privo di fisicità) per il godimento, da parte di un altro soggetto, evoca l'idea del contratto di loca-

---

zione" affermando che: "*Sulla base di quanto ad oggi valutabile riguardo la qualificazione giuridica del contratto di cloud computing, con particolare riferimento alla tipologia SaaS, e considerata l'attuale assenza di specifiche disposizioni normative e interpretazioni giurisprudenziali al riguardo, si ritiene che la qualificazione giuridica dei contratti in esame più convincente sia quella di un appalto di servizi disciplinato dalle disposizioni del codice civile applicabili anche in caso di appalti pubblici di servizi, come espressamente previsto dalle disposizioni del Codice degli appalti (D. Lgs. 163/2006)*".

[26] Si veda MANCARELLA M., cit., p. 217

[27] Così Tribunale di Napoli, Sent. del 26.2.2002.

zione e induce a pensare che il negozio in esame sia riconducibile alla disciplina dettata dal codice civile agli artt. 1571 e ss.

In effetti, la fattispecie del contratto di *hosting* presenta molte coincidenze con la locazione ed una loro sovrapposizione non è da escludere a priori. Sussiste, però, un elemento che conduce, nuovamente, verso un altro tipo negoziale: l'appalto di servizi. Infatti lo spazio concesso in godimento non è una risorsa informatica ben determinata e, al contrario, è spesso soggetta a variazione. Il fornitore è obbligato a garantire livelli di servizio e per far ciò può anche modificare la dislocazione dello spazio virtuale concesso in godimento. Così, l'inadempimento si verifica quando il fornitore non è in grado di garantire i servizi (spazio, accesso, connessione ecc) e non quando lo spazio logico concesso è soggetto a migrazione da una piattaforma ad un'altra equivalente.

La tipologia più diffusa di questa fattispecie negoziale è il servizio di *web-hosting*, che consiste nella concessione di uno spazio logico ove viene alloggiato un sito *web*[28].

La seconda specie di locazione di spazio *web* è il summenzionato contratto di *housing*, che consiste nella presa in carico e, eventualmente, nella gestione (cosiddetta *management*) di componenti *hardware* del cliente: "*[…] la proprietà dell'*hardware *e del* server *e la sua configurazione permangono in capo al titolare del sito […]*"[29]. Il *cloud provider* il titolare del sito mette in condizione di connettersi alla rete telematica dal lato *server* e offre servizi complementari, come ad esempio la manutenzione e l'assistenza tecnica, di cui si tratterà più avanti.

Dal presente negozio, nascono, in capo al prestatore di servizi, distinti tipi di obbligazione. Vi è, in primo luogo, l'obbligo di mantenere una connessione secondo le modalità previste dall'accordo contrattuale, che si configura come obbligazione di mezzi. Contemporaneamente sorge l'obbligo di custodia delle apparecchiature di proprietà del titolare del sito, che, invece, si configura come obbligazione di risultato del tutto assimilabile a quella che nasce da un contratto di deposito (nel quale l'obbligazione principale è costi-

[28] In tale ipotesi è sicuramente predominante la fornitura di uno spazio virtuale dove collocare le pagine *web* e dunque la natura giuridica di tale contratto può essere ravvisata nella locazione di beni mobili, denominata anche noleggio

[29] Tribunale di Napoli cit. 2002.

tuita dall'obbligo di custodia e di restituzione in natura dell'oggetto della prestazione).

Un esempio specifico di servizi complementari al contratto di *housing* sono il *back-up* ed il *disaster recovery*; si tratta di servizi autonomi, l'uno dall'altro, ma strettamente connessi e per tale ragione quasi sempre conviventi in un unico negozio. Tramite questo servizio, il fornitore compie il salvataggio periodico di tutti i dati, i programmi (comprese le configurazioni) contenuti negli apparati del cliente al fine di garantire la continua disponibilità, anche in presenza di avaria al sistema informatico del cliente.

La fattispecie negoziale in esame può essere inquadrata nell'ambito dell'appalto di servizi o del contratto di opera a seconda della qualità del fornitore del servizio: se si tratta di un'impresa che si impegna a realizzare il servizio con la propria organizzazione di mezzi e personale ovviamente si stipulerà un contratto d'appalto, mentre se si tratta del singolo professionista o di un gruppo di professionisti associati si concluderà un contratto di opera, nel quale prevale il lavoro personale.

Negli ultimi anni, il *back-up* ed il *disaster recovery* sono divenuti di vitale importanza, anche in ragione di quanto imposto dalla disciplina dettata in materia di protezione dei dati personali, della quale si è già trattato nella parte quarta.

2.4 *Cloud* e *outsourcing* a confronto

Il rapporto negoziale che si instaura tra il *cloud provider* e il fruitore del servizio spesso è accostato al cd. *outsourcing*[30]. Con questo termine si indica il processo di esternalizzazione delle attività di un'impresa (pubblica o pri-

[30] Cfr. MANTELERO A., *Processi di* Outsourcing *informatico e* cloud computing*: la gestione dei dati personali ed aziendali* Saggi, in Dir. Informaz.informat., 2010, pp. 673 e ss. Per un eventuale approfondimento circa i contratti funzionali alla gestione dei processi di *outsourcing* informatico si vedano: TOSI F., *Il contratto di* outsourcing *di sistema informatico*, Milano, 2001; PITTALIS M., Outsourcing*, in Contratto e Impresa*, 2000, pp. 1010 ss.; MUSELLA A., *Il contratto di* outsourcing *del sistema informativo*, in Dir. informaz. informat., 1998, pp. 857 ss.; CARDARELLI F., *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d.* outsourcing, in Dir. informaz. informat., 1993, I, pp. 85 ss.

vata) le quali vengono affidate e svolte all'esterno da soggetti terzi[31]. Non trattandosi di un negozio tipizzato[32], i tentati di riconduzione agli schemi codicistici conducono, ancora una volta verso il contratto dell'appalto di servizi[33].

---

[31] La cessazione di un'attività (per es. la gestione del sistema informativo aziendale) sino a quel momento svolta all'interno dell'azienda e la sua acquisizione sul mercato esterno, sotto forma di servizio (cosiddetta esternalizzazione) è soltanto una delle forme dell'*outsourcing*, conosciuta come "*simple outsourcing*" o anche come "*direct third party outsourcing*". Come osservato da MANTELERO A., op cit., pp. 674 e ss. "*è questo il modello di* outsourcing *(c.d.* direct third party outsourcing*) che qui interessa, poiché ad esso fanno principalmente riferimento le operazioni che vedono il ricorso al* cloud computing". Seppur non d'interesse in ambito *cloud*, per mere ragioni di completezza, è utile ricordare le altre tre forme negoziali annoverabili sotto l'etichetta di *outsourcing*: "*transfer outsourcing*", nel quale un'impresa trasferisce al fornitore del servizio la piena proprietà dell'intero ramo di azienda che si occupa della gestione del proprio sistema informativo (questo differisce dal "*simple outsourcing*" che, al contrario, come detto non comporta alcun trasferimento di settori aziendali); "*joint-venture outsourcing*", nel quale l'intero settore informatico dell'azienda viene trasferito a favore di una società mista, il cui capitale è suddiviso tra cliente e fornitore secondo gli schemi tipici della *joint-venture*; "*group outsourcing*", che è una variante del precedente, caratterizzato dal fatto che la società a favore della quale è stato attuato il trasferimento del ramo di azienda rimane interamente controllata dal cliente. Con riferimento ai processi di *outsourcing* nel settore ICT in generale, oltre che al *cloud computing*, si veda anche POLITECNICO DI MILANO – DIPARTIMENTO DI INGEGNERIA GESTIONALE, *ICT Strategic Sourcing: nuovi equilibri oltre la crisi*; Rapporto 2009 Osservatorio ICT Strategic Sourcing, novembre 2009, in http://www.osservatori.net.

[32] Secondo autorevole dottrina, l'*outsourcing* rileva sotto il profilo funzionale ed organizzativo e non quale modello contrattuale o autonoma categoria giuridica; cfr. CARDARELLI F., *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, in Dir. Inf. Inform. 1993, I, 86, secondo cui tale termine "*non può avere alcuna rilevanza giuridica*"; cosı` anche PITTALIS M., Outsourcing, in Contr. e impr., 2000, 1006 s. Sui profili contrattuali della gestione del processo di outsourcing si vedano: F. TOSI, *Il contratto di outsourcing di sistema informatico*, Milano, 2001; M.PITTALIS, op. cit., 1010 ss.; A. MUSELLA, *Il contratto di* outsourcing *del sistema informativo*, in Dir. Inf.Inform., 1998, 857 ss.; F. CARDARELLI, op. cit., 85 ss.

[33] Sebbene i processi di esternalizzazione siano regolati attraverso una varietà di modelli contrattuali, nell'ambito, invece, dell'acquisizione del servizio erogato dall'*outsourcee*, il rapporto sussistente fra le parti risulta solitamente riconducibile al contratto di appalto di servizi, come spesso avviene anche nelle ipotesi di *cloud computing*. Cfr. in dottrina: CAGNASCO O., COTTINO G., *Contratti commerciali*, in *Trattato di Diritto Commerciale* diretto da G. COTTINO, Padova, 2000, p. 353; M. PITTALIS, *Outsourcing*, cit., p. 1015 ss.; A. MUSELLA , *Il contratto di outsourcing del sistema informativo*, cit., pp. 859 ss.; F. CARDARELLI, *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d. outsourcing*, cit., p. 94.

Rinviato a quanto già detto, nei precedenti paragrafi, a proposito della riconduzione di alcune forme di *cloud computing* al contratto di appalto di servizi, in questa sede si illustreranno brevemente le principali somiglianze e differenze tra quest'ultimo e il contratto di *outsourcing*[34].

In primo luogo, come già detto sia nel contratto di *cloud computing* che in quello di *outsourcing* (nella forma *simple*), lo scopo perseguito dalle parti consiste nell'esternalizzazione (totale o parziale) della gestione delle attività o dei servizi. Non a caso gli schemi contrattuali di entrambe sono strutturati mantenendo la predominanza e la centralità del servizio offerto e della qualità dello stesso. Da ciò consegue che, sia nel contratto di *cloud computing* che in quello di *outsourcing*, sono attentamente curati gli aspetti inerenti gli *standard* per l'esecuzione delle prestazioni previste nell'accordo, la predisposizione degli indici e dei parametri per la misurazione dell'efficienza dei servizi e per la determinazione dei costi. Affinché le prestazioni e i parametri così determinati siano vincolanti per la parte fornitrice dei servizi, questi aspetti tecnici sono inseriti all'interno di allegati appositi che, insieme alle clausole contrattuali inserite nel documento principale, vanno a comporre la complessa articolazione dei contratti del *cloud*.

Per quanto concerne le differenze, mentre nel contratto di *outsourcing* tendenzialmente si realizza l'esternalizzazione sia delle risorse strutturali che umane, nei contratti del *cloud* prevalgono i profili di organizzazione dei servizi di *computing* e non la dislocazione di risorse umane.

Infine, con particolare riferimento al *public cloud*, i servizi sono offerti da un unico *cloud provider* verso una moltitudine di fruitori attraverso la predisposizione di contratti *standard*. Nell'*outsourcing*, invece, tale schema di erogazione non è presente, in quanto fra le parti contrattuali vige un rapporto paritario, in cui solitamente i servizi pattuiti sono frutto di una negoziazione particolare e dettagliata, personalizzata sulla base delle esigenze delle parti.

[34] Vedi sul punto MANTELERO A., *Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali*, Saggi, in Dir. Informaz. informat., 2010, pp.682 e ss.

2.5 La centralità dei dati come elemento di classificazione negoziale: il contratto di deposito di beni digitali

Una parte della dottrina[35], discostandosi totalmente dagli orientamenti sopra illustrati, parte dall'assunto che il contratto di *cloud* consiste principalmente nella gestione della circolazione dei beni digitali (cioè dei dati) per conto dell'ente pubblico o privato che si rivolge al *cloud provider*. In altri termini il contratto consiste nell'affidare, al fornitore del servizio, i beni digitali da custodire mediante deposito.

In base all'art. 1766 c.c. "*Il deposito è il contratto con il quale una parte* (depositario) *riceve dall'altra* (depositante) *una cosa mobile con l'obbligo di custodirla e restituirla in natura*".

Il primo problema da porsi, per verificare se effettivamente di deposito si tratta, è quello di capire se i dati digitali possano essere annoverati tra i beni mobili di cui all'art. 812, comma 3, c.c.. Il passo immediatamente successivo è quello di accertare la loro natura fungibile o infungibile, in quanto il contratto di deposito (regolare) ha per oggetto una cosa infungibile (la cosa deve essere conservata, custodita e restituita in natura); quando, invece, il bene depositato è fungibile (per esempio il denaro) allora si parla di deposito irregolare (art.1782), con facoltà del depositario di servirsi della cosa (di cui acquista la proprietà) e con l'obbligo, per lo stesso soggetto, di restituirne altrettante della stessa specie e qualità.

Quanto al primo punto, i beni dell'informazione sembrano essere conformi alla definizione residuale di bene mobile contenuta nel codice civile ma questa prima constatazione trova immediata smentita nella voce di chi esclude che oggetto del deposito possano essere beni immateriali[36]. La stessa dottrina, però, precisa che possono essere oggetto di deposito i beni che siano suscettibili di immagazzinamento e conservazione. Così, nel tentativo di trovare concordanza tra tutte le posizioni, si potrebbe affermare che non sono idonei al deposito quei beni immateriali che, in assoluto, non possono es-

[35] PROSPERETTI E., *L'opera digitale tra regole e mercato*, 2013, pp. 262 ss.

[36] Cfr. IVONE V., *Commento all'art. 1766*, in Dei singoli contratti, vol. II, in Commentario al Cod. Civ. diretto da E. Gabrielli, 2011, p. 775.

sere immagazzinati quali, ad esempio, le energie naturali, mentre i beni digitali dell'informazione (i dati) sono, a contrario, idonei al deposito.

Rimane, ora, da stabilire se il deposito *cloud* sia regolare o irregolare. In tal senso si consideri che i dati che costituiscono il bene digitale dell'informazione, nel momento in cui vengono restituiti, non sono esattamente gli stessi che sono stati depositati. Ciò vale dal punto di vista strettamente tecnico-informatico, in quanto i dati elaborati (cioè letti da varie posizioni/applicazioni e trasmessi da diverse reti telematiche) mutano continuamente anche se rimangono equivalenti nel loro significato intelligibile all'uomo. In conseguenza di ciò, i beni digitali depositati nella nuvola si presentano con caratteristiche di infungibilità e quindi oggetto di deposito irregolare.

In senso opposto, va però attentamente considerato che il *cloud provider*, depositario dei beni digitali dell'informazione, non può servirsi, né diventare proprietario, dei dati che custodisce e che appartengono al depositante. Anzi, come si è avuto modo di approfondire nella parte terza del presente lavoro, chi eroga il servizio di *cloud* ha precisi obblighi di riservatezza sugli stessi (ancor più se si tratta di dati sensibili, come quelli sanitari), che provengono direttamente dalla legge, ancora prima che dal regolamento negoziale[37]. Ciò accomuna il contratto di *cloud computing* al deposito regolare.

Ancora una volta ci si trova a non poter esattamente incasellare il contratto di *cloud computing* in alcuna delle fattispecie negoziali tipiche contenute nel codice civile. Il deposito *cloud*, se di deposito si tratta, è di natura *sui generis*, quindi atipico, che segue principalmente la disciplina del deposito regolare, fino a sconfinare, seppure per risibili aspetti, nel deposito irregolare. È fuor di dubbio, infatti che l'obbligazione del depositario in *cloud*, che

[37] Si può parlare di perfetta coincidenza con il deposito irregolare, anche per la parte relativa alla proprietà dei dati depositati, nel caso di *social network*, come ad esempio Facebook, che chiaramente prevede nelle proprie condizioni generali la possibilità di servirsi dei dati che gli sono stati comunicati, fin tanto che il profilo rimane attivo. Solo con l'eliminazione del profilo (e di eventuali dati caricati in altri profili) si restituisce la piena titolarità al depositante. Su questi aspetti, si veda COGO A., *Le regole del contratto tra* social network *e utente sull'uso della proprietà intellettuale del gestore, dell'utente e degli altri utenti – riflessioni a partire dall'individuazione del fenomeno, dei suoi soggetti e della funzione del contratto*, in AIDA, 2011, 342 ss.; PROSPERETTI E., *La condivisione* one-click *di dati di terzi verso piattaforme Internet e le regole della* privacy, in Rivista di Diritto, Economia e Tecnologie della Privacy, 1, 2013.

si riserva la facoltà di modificare la ubicazione, spostare, archiviare in vario modo i dati è quella di restituire, quando richiesto, beni digitali della stessa natura e specie ricomponendo gli archivi.

Il depositante, dal canto suo, conserva la titolarità dei propri dati, che, nonostante siano archiviati sulle memorie del depositario, non divengono mai di proprietà di quest'ultimo[38]. Del pari i dati depositati da diversi titolari, raggruppati nella massa dei dati archiviati nei *server* del *cloud provider* (cd. *multitenancy*) non creano alcuna comunione *pro indiviso* tra i vari depositanti che convivono, appunto, nello stesso archivio. A ciò si aggiunga che la titolarità sul dato non significa necessariamente proprietà ma anche semplicemente possesso, così da rendere (relativamente a quest'aspetto) il contratto di *cloud* pienamente compatibile con il contratto di deposito. Diversa dal deposito è la cessione, per la quale sono necessari pieni diritti sul bene ceduto. É possibile depositare beni digitali (dati, informazioni) anche di proprietà di terzi e di cui si ha la mera custodia purché la memorizzazione di tali informazioni non comporti violazione di legge.

La riconduzione al contratto di deposito, e quindi alla sua disciplina, comporta anche l'applicazione del regime di responsabilità, che le è propria, al contratto di *cloud*, in relazione, ad esempio, all'impossibilità sopravvenuta di mantenere l'informazione digitale in deposito con conseguente perimento.

In base alle disposizioni codicistiche, il depositario deve: custodire la cosa; usare nella custodia la diligenza del buon padre di famiglia; non servirsi della cosa depositata; non dare la cosa depositata ad altri; restituirla a richiesta o al termine convenuto; restituire i frutti della cosa che egli abbia percepiti. Da tali obbligazioni discende che la responsabilità contrattuale del depositario (e quindi anche quella del *cloud provider*) verte su tre principali aspetti: custodia, diligenza e conservazione della cosa. La valutazione, più o meno rigorosa, di tale responsabilità è strettamente connessa alla misura del corrispettivo di un contratto che, così come è stato tipizzato, si presume a titolo gratuito.

Non si può certamente pensare che il contratto di *cloud* possa affermarsi, e quindi diffondersi, nel mercato a titolo gratuito, visto che la qualità e la sicurezza, che ne sono alla base, comportano investimenti notevoli per chi si impegna ad assicurarle. Pertanto, la diligenza attesa sarà, così, tanto maggio-

[38] Sulla titolarità dei dati si veda il successivo paragrafo.

re, quanto più stringenti saranno i parametri di qualità e sicurezza fissati in contratto. Parallelamente, il costo che dovrà sostenere la Pubblica amministrazione, per fruire dei servizi di *cloud*, varierà al variare degli *standard* garantiti in accordo dal depositario dei dati digitali.

Tra gli obblighi del fornitore, va certamente contemplata la necessità di inserire nel regolamento contrattuale la garanzia di interoperabilità, così da soddisfare l'obbligo di restituzione tipico dei contratti di deposito. Se, al contrario, i dati sono detenuti al di fuori degli *standard* di interoperabilità, e quindi resi fruibili soltanto attraverso procedure proprietarie mediate dal depositario, una parte dei diritti tipici del depositante verrebbe compromessa. Si pensi, ad esempio, all'impossibilità di ispezionare i dati alloggiati sulla "nuvola", senza il consenso del depositario, che si traduce in una forte limitazione del diritto d'accesso. Si pensi, altresì, al pericolo di mancata restituzione futura dei beni depositati, che si configurerebbe nel caso di restituzione di dati "illeggibili" (per via della detenzione in formato non interoperabile). L'interoperabilità, al di la del suo risvolto pratico, garantisce il diritto del titolare dell'informazione digitale a conseguire l'accesso ai beni custoditi in una infrastruttura informatica attrezzata.

Quando il bene digitale in deposito è l'informazione sanitaria, l'interoperabilità va ben oltre le modalità in cui alcuni servizi possono essere rilasciati all'interno di un singolo sistema sanitario e, in un senso più ampio, ha a che vedere con le migliori pratiche per la rappresentazione dell'informazione e per la sua fruizione per assolvere a finalità di cura e assistenza, tipiche degli esercenti le professioni sanitarie, e quindi per garantire il diritto alla salute.

Il rischio di non potere accedere facilmente al dato sanitario in *cloud* ovvero di non ottenere il suo immediato rilascio in formato leggibile al momento della cessazione degli effetti del contratto di *cloud* è un grande rischio che non può essere corso. Le parti, quindi, nella predisposizione dell'autoregolamento che disciplina il rapporto di deposito in *cloud*, possono avvalersi della libertà contrattuale ed inserire le clausole di garanzia per la tenuta e per il rilascio dei dati in formato interoperabile. La mancata previsione di questi aspetti può comportare un serio pregiudizio al titolare dei dati digitali, il quale, fermo il diritto alla restituzione, non potrà pretendere la

leggibilità (quale atto dovuto) dei dati sanitari restituiti, con tutto ciò che ne consegue.

3. Profili strutturali e contenutistici

Il contratto di *cloud computing*, nelle sue molteplici forme, si presenta sempre come fattispecie complessa ed eterogenea. Dal punto di vista strutturale, considerando come si sta diffondendo nella prassi commerciale, consta di tre distinti documenti[39]: nel primo sono previste le condizioni generali di servizio, nel secondo sono elencate le regole di comportamento che le parti si impegnano a rispettare (dette anche *policies*) e, infine, nel terzo sono descritte le modalità di trattamento dei dati personali[40].

Relativamente ai contenuti, l'atipicità che lo caratterizza impone alle parti di disciplinare tutti quegli aspetti che potrebbero rappresentare un'incognita e quindi generare contenziosi, o complicarne la soluzione quando sono già sorti, se non vengono puntualmente regolamentati. Si tratta, in primo luogo, di aspetti generali relativi alla durata, alla lingua, al corrispettivo, alla legge applicabile ed alla competenza giurisdizionale ma anche alle modalità di gestione delle informazioni e dei dati inseriti nel *cloud* (principalmente, protezione, trasferimento e riservatezza).

[39] Sono stati esaminati i modelli contrattuali adottati, ad oggi, dai principali fornitori di servizi di *cloud computing*,. Una più estesa indagine, è stata condotta nel 2010 dalla Queen Mary University of London, School of Law, cfr. BRADSHAW – MILLARD - WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, 1 September 2010, in http://ssrn.com.

[40] Così A. MANTELERO nella relazione: "*Il* cloud computing*, inquadramenti giuridici e differenze di approccio contrattuale*" tenuta dall'autore al convegno di Milano del 17 gennaio 2012: "Cloud Computing - *I diversi approcci contrattuali e nuove definizioni in ambito* privacy". L'audio di tale intervento e la relativa presentazione sono fruibili *on-line*.

3.1 Profili soggettivi: titolarità del dato e responsabilità connesse

L'elemento caratterizzante il *cloud computing*, qualunque sia la configurazione negoziale, è quella del trasferimento di dati (anche ma non necessariamente di carattere personale[41]) tra il soggetto (pubblico o privato) che acquista il servizio e il *cloud provider*.

A tale flusso, con riferimento al rapporto tra l'informazione digitale ed i soggetti coinvolti, compie espresso riferimento l'art. 58, comma 1, del D. Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale o semplicemente CAD), il quale dispone che: "*il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato*".

La titolarità sul dato digitale, nel significato qui inteso, è riconducibile tanto al soggetto che lo ha creato a titolo originario, quanto a colui che lo ha raccolto, dal primo redattore, e poi lo ha trasferito. L'accezione di titolare è ampia e non si riferisce esclusivamente al proprietario dell'informazione digitale ma anche a chi ne ha semplicemente il possesso. Inoltre, tenuto conto che il flusso di dati trasferiti non è esclusivamente di natura personale, il titolare del dato non coincide necessariamente con il titolare del trattamento dei dati personali[42] contemplato dal D. Lgs. 30 giugno 2003, n. 196 (e anche dal Regolamento UE 2016/679).

In ambito sanitario, data la delicatezza e natura delle informazioni trattate, il corretto inquadramento della titolarità sul dato assume particolare im-

[41] Nel presente paragrafo si tratta di dati intesi come informazioni digitali di qualunque natura, anche non personale. La nomenclatura utilizzata, relativamente ai dati ed ai soggetti, pertanto non è quella dell'art. 4 del D.lgs. 196/03 (e del Regolamento UE 679/2016). Dei rapporti soggettivi relativamente al trattamento dei dati personali, si è già detto nella parte quarta, alla quale si rinvia anche per una lettura parallela finalizzata a comprendere la diversa prospettiva di analisi.

[42] La titolarità di tale soggetto è relativa alle attività di trattamento, mentre la titolarità di cui qui si tratta è relativa alla posizione giuridica soggettiva sul bene digitale (dato), che può essere un vero e proprio diritto soggettivo ma può anche riferirsi semplicemente alla posizione di possessore. In alcuni casi, il titolare del trattamento ed il titolare del dato possono coincidere. Non si confonda, però, la titolarità, sul dato, tipica dell'interessato al trattamento dei dati personali, che è colui al quale il dato si riferisce e non colui che ha creato il dato (come, ad esempio, nel caso della Pubblica Amministrazione sanitaria che genera un referto medico).

portanza in termini di responsabilità sulla sua sicurezza, esattezza e veridicità. La fattispecie diventa particolarmente problematica quando il contratto contiene clausole volte ad attribuire al fornitore del servizio il diritto di utilizzare, anche a fini commerciali[43], i dati gestiti all'interno dei propri *servers* ovvero disposizioni che, a vario titolo, ne limitano le responsabilità. Tale prassi, purtroppo, non è insolita nel mercato dei servizi di *cloud computing*, ove, come si è già avuto modo di illustrare, spesso non esistono trattative e i contratti sono predisposti (quindi imposti) dai *cloud providers*. In tali fattispecie si presenta particolarmente debole la posizione del titolare che accetta servizi di *cloud computing* gratuiti, a fronte di un uso molto libero dei dati gestiti in remoto.

Si consideri, inoltre, che l'esternalizzazione e la delocalizzazione dei dati, mediante gli accordi dal contenuto sopraccitato, comportano la perdita del controllo diretto sugli stessi. Infatti, nell'ipotesi in cui vi siano dei guasti alla rete o, più in generale, dei malfunzionamenti (qualunque sia il tipo di servizio offerto), si potrebbe determinare l'indisponibilità, l'inacessibilità o, addirittura, la perdita dei dati, con conseguente responsabilità del fornitore del servizio per i danni causati.

La problematica suddetta è evidenziata anche nel vademecum su "*cloud e sanità*" (di Federsanità-ANCI è Istituto Italiano Privacy del 2013), già presentato nella parte terza, nel quale si suggeriscono alcuni correttivi, tra cui quello di procedere al salvataggio *in house* di una copia dei dati gestiti in *cloud*, anche laddove non siano personali, ma dalla cui perdita o indisponibilità possano derivare danni economici, all'immagine o, in generale, relativi alla missione e alle finalità perseguite. Una tale situazione, però, mortifica le potenzialità del *cloud computing*, che dovrebbe liberare il fruitore del servizio da tutti gli oneri relativi alla custodia e sicurezza delle informazioni digitali.

Una soluzione più agevole potrebbe essere quella che agisce esclusivamente a livello negoziale, senza caricare, come nella predetta soluzione, il

[43] Si presenta particolarmente debole la posizione del titolare che accetta servizi di *cloud computing* gratuiti per la gestione di dati testi e materiali multimediali (foto e video), ma senza alcuna possibilità di negoziazione delle clausole. In tali casi, sempre secondo Belisario, le amministrazioni devono valutare con estrema attenzione la tipologia dei dati, che una volta inseriti nella nuvola, non potranno più essere sotto il diretto controllo dell'utente.

titolare di compiti dei quali si è spogliato (o ha cercato di spogliarsi) con il contratto di *cloud*.

Per far fronte a problemi di questo tipo sarebbe opportuno, quindi, inserire nell'accordo con il *provider* i cosiddetti SLA (*Service Level Agreement*), mediante i quali si tenta di ottenere la misurazione, oggettiva e numerica, dei risultati raggiunti dal fornitore. Tipicamente, i parametri da considerare per tali misurazioni, sono i tempi di intervento assicurati dal fornitore a partire dalla chiamata del cliente, i tempi di risoluzione dei guasti, la percentuale di soluzione dei guasti, la percentuale di difettosità, il tempo medio tra due guasti consecutivi (*MTBF*, cioè *Mean Time Between Failures*) dell'impianto, nonché la continuità operativa e il *disaster recovery*[44]. É, altresì, consigliabi-

[44] Quando il *cloud computing* è adottato in ambito pubblico, la previsione di garanzia dei livelli di servizio e di sicurezza, di continuità operativa e di è *disaster recovery* sono previste dalla legge. In particolare, l'Art. 68, co. 1-bis, lett. c, del Codice dell'Amministrazione Digitale, dispone che: "*[…] le pubbliche amministrazioni prima di procedere all'acquisto, […] effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri: […] c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito*". La continuità operativa e il *disaster recovery*, sono stati introdotti, con il D.Lgs 235/2010, che ha novellato il CAD con l'art. 50-*bis*. In base ad esso è divenuto obbligatorio per le Pubbliche Amministrazioni italiane la definizione di:
"*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* ".
Sul *disaster recovery* in ambito pubblico si vedano anche le "*Linee guida per il* disaster recovery *delle pubbliche amministrazioni ai sensi del c. 3, lettera b) dell'art. 50*bis *del Codice-dell'Amministrazione Digitale*" pubblicate da AgID, la cui versione aggiornata al 2013 è consultabile al seguente link: http://www.agid.gov.it/sites/default/files/linee_guida/linee-guida-dr.pdf.
Alle garanzie di fonte legale di cui sopra, se ne può aggiungere un'altra di portata più generale, in quanto la sua applicazione non è limitata al settore pubblico. Si tratta dell'obbligo di notifica-

le inserire specifiche clausole che contemplino la responsabilità del fornitore in caso di inadempimento degli obblighi contrattuali di affidabilità.

Un ulteriore aspetto critico, peraltro già affrontato nel paragrafo dedicato al contratto di deposito di dati digitali, è rappresentato dalla portabilità dei dati verso altre piattaforme. Con questo termine si vuole indicare l'idoneità dei formati e delle tecnologie utilizzate da un fornitore di servizi ad essere utilizzabili da altri fornitori, senza che ciò comporti la perdita di informazioni o, addirittura, l'impossibilità di utilizzo delle stesse. Data la delicatezza e l'importanza del problema, per far fronte al crescente uso delle tecnologie proprietarie da parte dei *cloud provider* che favoriscono il sorgere di problemi di portabilità, il legislatore ha previsto un obbligo per le Pubbliche Amministrazioni che utilizzano programmi sviluppati *ad hoc* per conto e a spese delle stesse, di prevederne la portabilità su altre piattaforme, al fine di favorire il riuso dei programmi informatici[45]. Alla luce di ciò, nei contratti tra i fornitori di servizi in *cloud* e le amministrazioni sanitarie e, prima anco-

---

re al Garante le ipotesi di violazione dei dati personali in seguito al verificarsi di un incidente informatico (*data breach*). Tale obbligo è stato inserito, per la prima volta, limitatamente all'ambito delle "comunicazioni elettroniche", dal D. lgs. 69/2012 (con il quale è stato introdotto l'art. 32-*bis* del D.lgs. 196/03). Oggi il suddetto obbligo è stato esteso anche ad altri ambiti, quindi anche ai servizi cloud, con gli articoli 33 e 34 del Regolamento UE 679/2016. Essi dispongono che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'Autorità di controllo senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata. L'art. 34, invece, prevede un'altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all'interessato. Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione all'interessato non è dovuta se: a) il responsabile del trattamento ha utilizzato le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura, oppure b) il responsabile del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1, oppure c) detta comunicazione richiederebbe sforzi sproporzionati. In una simile circostanza, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

[45] Art. 69, comma 2, D. Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale)

ra, nei capitolati di appalto o nelle specifiche di progetto, si dovrebbe inserire l'esplicito obbligo di adottare standard internazionali per la codifica dei dati sanitari e, così, garantire l'utilizzabilità degli stessi anche presso un diverso fornitore del servizio.

3.2 La legge applicabile

Quando il *cloud computing* coinvolge attori situati in Paesi diversi (e quindi in ordinamenti diversi), si pone il problema della disciplina applicabile a quel rapporto, soprattutto in caso di controversie. Può accadere, addirittura, che il prestatore del servizio sia localizzato in territorio extra-europeo. La questione è assai delicata, soprattutto alla luce della già citata tendenza alla standardizzazione delle clausole contrattuali da parte dei *cloud provider*[46].

Tra gli scenari ipotizzabili, si pensi, tra i tanti, al caso in cui si rivendichi la proprietà (o, in generale, la titolarità, intesa nel senso anzidetto) di un documento prodotto o memorizzato in un'infrastruttura *cloud*, oppure al caso della garanzia applicabile quando il contratto è stipulato con un fornitore avente sede in un luogo diverso da quello in cui sono situate le "nuvole" informatiche ove risiedono i dati.

In fattispecie come queste, risulta alquanto problematico il dover stabilire, a posteriori, il diritto applicabile al caso concreto. Spesso, infatti, il divario e la differenza di tutele, tra i diversi ordinamenti, potrebbe essere talmente elevato da vanificare i benefici i vantaggi (anche in termini economici) della scelta di soluzioni di *cloud computing*[47]. Per questa ragione è opportuno che i protagonisti dei contratti di *cloud* (soggetti pubblici o privati) de-

[46] Così MANTELERO A., *Il contratto per l'erogazione dei servizi di* cloud computing, in Contratto e Impresa 4-5/2012 , pp. 1221 e ss., il quale osserva che: "*anche qualora venisse prescelta la legge italiana, potrebbero comunque emergere delle difficoltà interpretative, stante la predisposizione dei testi contrattuali sulla base di modelli statunitensi. In alcuni casi il ricorso ad istituti e concetti giuridici di* common law *può infatti risultare non agevolmente compatibile con la qualificazione degli stessi alla luce dell'ordinamento nazionale*". Per una più ampia disamina di questi aspetti si veda DE NOVA, Il contratto alieno, Torino, 2010.

[47] Così BELISARIO E., "Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli - eBook n.17, Altalex 2011, pag. 13 e ss.

terminino, *ex ante*, con certezza la disciplina che si applicherà a quello specifico rapporto.

In Italia, la disciplina di riferimento è la L. 31 maggio 1995 n. 218, recante "*Riforma del sistema italiano di diritto internazionale privato*" il cui art. 57, in tema di obbligazioni contrattuali, rinvia espressamente alle norme di cui alla Convenzione di Roma del 19 giugno 1980[48], così come novellata dal Regolamento CE 593/2008; per la competenza giurisdizionale, invece, sempre per espresso richiamo della suddetta Legge[49], la fonte di riferimento è la Convenzione di Bruxelles

Le parti, in primo luogo, secondo il principio generale, sancito dall'art. 3 del reg. CE 593/2008, hanno libertà di scelta[50] della legge applicabile al contratto. Tale libertà, in considerazione del carattere universale del Regolamento (art. 2), può estendersi fino alla scelta della legge uno Stato che non è parte dell'Unione europea oppure di più leggi nazionali diverse[51].

La scelta operata dalle parti diventa il parametro di riferimento relativamente all'interpretazione della volontà negoziale, all'esecuzione delle obbligazioni che ne discendono e alle conseguenze per l'inadempimento delle stesse, al risarcimento di eventuali danni, all'estinzione delle obbligazioni nate per effetto di quel rapporto e, infine, alle conseguenze delle cause di in-

[48] La Convenzione è stata resa esecutiva con la legge 18 dicembre 1984, n. 975

[49] L'art. 3 così recita: "*La giurisdizione sussiste inoltre in base ai criteri stabiliti dalle sezioni 2, 3 e 4 del titolo II della Convenzione concernente la competenza giurisdizionale e l'esecuzione delle decisioni in materia civile e commerciale e protocollo, firmati a Bruxelles il 27 settembre 1968, resi esecutivi con la legge 21 giugno 1971, n. 804, e successive modificazioni in vigore per l'Italia, anche allorchè il convenuto non sia domiciliato nel territorio di uno Stato contraente, quando si tratti di una delle materie comprese nel campo di applicazione della Convenzione*."

[50] Sebbene non venga richiesto che tale scelta sia espressa in forma scritta, è sempre consigliabile farlo per questioni probatorie, in quanto, in caso contrario, per essere fatta valere, dovrà risultare in modo ragionevolmente certo dalle disposizioni del contratto o dalle circostanze del caso (art. 3 del Regolamento CE 593/2008).

[51] La scelta di più leggi combinate è meglio nota con il nome di "*depeçage*" (frazionamento) o "*morcellement*", in quanto presuppone la scomposizione del contratto in più parti ed il conseguente assoggettamento di ciascuna di esse a leggi nazionali diverse. Rinviando ad altra sede più appropriata l'approfondimento della questione, si vogliono qui semplicemente evidenziare i limiti di una tale tecnica di combinazione che potrebbe essere inficiata dall'assenza di armonia tra le fonti scelte dalle parti, in quanto appartenenti ad ordinamenti spesso molto diversi nelle regole e nei principi.

validità che dovessero presentarsi. L'art. 3 del Regolamento prevede anche la possibilità di modificare, di comune accordo, la legge precedentemente scelta come regolatrice del contratto, o di effettuare tale scelta anche in un momento successivo alla conclusione del contratto.

Nell'opposto caso in cui le parti non operino alcuna scelta, l'art. 4 del regolamento, elenca una serie di esemplificazioni: legge del venditore, legge del prestatore di servizi, ecc. Osservando attentamente le fattispecie prese in considerazione, il comune denominatore è costituito dal fatto che, nel silenzio delle parti, si applica la legge del Paese dove non si esegue la prestazione pecuniaria.

Seppure non particolarmente rilevante per l'oggetto del presente lavoro, si ritiene opportuno fare un breve cenno, sempre a proposito della legge applicabile al *cloud* internazionale, all'ipotesi in cui il fruitore del servizio in *cloud* sia qualificabile come consumatore: l'art. 6 Regolamento CE 593/2008, fermo restando il principio generale di libera scelta della legge applicabile, dispone che il contratto tra un consumatore e un professionista è regolato dalla legge del Paese nel quale il consumatore ha la propria residenza abituale, a condizione che il professionista svolga le proprie attività commerciali o professionali, o le diriga con qualsiasi mezzo, nel Paese del consumatore. Pertanto, anche nel caso in cui siano realizzate forme di pubblicità in rete, ai contratti si applicherà la legge del Paese di residenza del consumatore. Nello stesso senso anche l'art. 143 del Codice del Consumo[52] il quale, in aggiunta, dispone che anche laddove le parti abbiano esercitato la propria scelta verso un Paese diverso da quello italiano, al consumatore devono comunque essere riconosciute le condizioni minime di tutela previste dal codice stesso[53].

---

[52] D. Lgs. 6 settembre 2005, n. 206 recante "*Codice del consumo, a norma dell'articolo 7 della legge 29 luglio 2003, n. 229*".

[53] In relazione ai profili che potrebbero interessare i contratti del *cloud computing*, la tutela minima riconosciuta dal Codice al consumatore prevede il rimedio processuale della cd. azione di classe ("*class action*"). In dottrina si ritiene che, per le caratteristiche tipiche dei servizi di *cloud computing*, i consumatori potrebbero beneficiare dell'azione collettiva prevista dall'art. 140-*bis*, D.Lgs. n. 206/2005. Si pensi, ad esempio, ad alcuni eventi come l'impossibilità temporanea di accedere alle risorse in *cloud* oppure al caso di diffusione o comunicazioni illecite di dati o informazioni degli utenti. Il danno cagionato da tali condotte agli utenti potrebbe essere tutelato attraverso l'azione suddetta.

L'art. 4, comma 1, lett. a) – h) del Regolamento n° 593/2008, al fine di individuare la legge applicabile, prende in considerazione anche un altro criterio, ossia il contratto è diversamente regolato a seconda della specifica tipologia negoziale tra quelle elencate. Di particolare interesse per il *cloud computing*, anche sulla base di quanto illustrato nei paragrafi precedenti, sono le fattispecie di "prestazioni di servizi" e di "contratto atipico". Quanto ai primi il contratto è disciplinato dalla legge del Paese nel quale il prestatore di servizi (*rectius* il *cloud provider*) ha la residenza abituale. Mentre, se il contratto non rientra tra quelli specificamente indicati dal Regolamento (contratto atipico), oppure si tratta di un contratto misto o complesso (cioè composto, allo stesso tempo, da diversi tipi contrattuali), si dovrà fare riferimento alla legge del paese nel quale la parte che deve fornire la prestazione caratteristica del contratto ha la residenza abituale.

3.3 Le clausole vessatorie

Come si è già avuto modo di evidenziare, l'esigenza di fornire un servizio standardizzato ad una molteplicità di fruitori comporta il ricorso a modalità di conclusione dei contratti che non prevedono la fase delle trattative. Questo scenario è frequente nei contratti di *public cloud*, dove, appunto, il rapporto è di uno a molti. Più raramente accade, invece, nei contratti di fornitura di servizi *cloud* personalizzati o "customizzati", in cui le parti concordano e bilanciano il contenuto dell'accordo.

L'assenza di trattative è spesso portatrice di clausole vessatorie che determinano uno squilibrio nel rapporto contrattuale, molto spesso a discapito del fruitore del servizio.

Nel contratto di *cloud* il fornitore, di regola, ha una posizione, di fatto, più forte della controparte, che in alcuni casi può essere anche formalmente inquadrata come parte debole, in quanto consumatore. In dette situazioni, la disciplina applicabile è quella contenuta nel codice del consumo (D.lgs. 6 settembre 2005, n. 206). L'art. 33, rubricato "*clausole vessatorie nel contratto tra professionista e consumatore*", considera vessatorie le clausole che "*[…] malgrado la buona fede, determinano a carico del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto*".

Sussiste, pertanto, una presunzione, *iuris tantum*, di vessatorietà per tutte quelle clausole che abbiano per oggetto, o per effetto, di "*escludere o limitare le azioni o i diritti del consumatore nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista*"[54].

L'inserimento di clausole considerate vessatorie, nel senso sopraddetto, comporta una nullità parziale del contratto: dette clausole sono nulle, mentre il contratto rimane valido per il resto.

I commi 4 e 5 dell'art. 34 sono di particolare interesse per i contratti di *cloud*, in quanto escludono la vessatorietà delle clausole (o degli elementi di clausola) che "*siano stati oggetto di trattativa individuale*". A ciò si aggiunga che, per i negozi conclusi mediante sottoscrizione di moduli o formulari (proprio come la maggior parte dei contratti di *cloud*) predisposti per disciplinare in maniera uniforme determinati rapporti contrattuali, "*incombe sul professionista l'onere di provare che le clausole, o gli elementi di clausola, malgrado siano dal medesimo unilateralmente predisposti, siano stati oggetto di specifica trattativa con il consumatore*".

Tuttavia, la possibilità di avere (e di dimostrare) la trattativa individuale sulle singole clausole dei contratti di *cloud*, stipulati con il consumatore, non trova grande applicazione, in quanto, spesso, le procedure di conclusione prevedono la sola registrazione dell'utente nel sito *web* del *cloud provider* senza alcuna trattativa in merito al contenuto del contratto e delle condizioni generali di servizio predisposte dal fornitore stesso.

---

[54] Il secondo comma dell'art. 33 del D.lgs. 206/2005, elenca le clausole che si presumono vessatorie fino a prova contraria. Rinviando al testo normativo per la consultazione del suddetto elenco, appare doveroso segnalare che, di recente sono state inserite due nuove ipotesi nell'elenco delle clausole che si presumono vessatorie. Esse sono:

"v-bis) imporre al consumatore che voglia accedere ad una procedura di risoluzione extragiudiziale delle controversie prevista dal titolo II-bis della parte V, di rivolgersi esclusivamente ad un'unica tipologia di organismi ADR o ad un unico organismo ADR;

v-ter) rendere eccessivamente difficile per il consumatore l'esperimento della procedura di risoluzione extragiudiziale delle controversie prevista dal titolo II-bis della parte V".

La novella è stata introdotta con il D.lgs. 6 agosto 2015, n. 130 *"attuazione del regolamento (UE) n. 524/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo alla risoluzione delle controversie online dei consumatori*", che si applicano a decorrere dal 9 gennaio 2016.

L'accordo tra le parti, però, non esclude la vessatorietà quando è volto a: "*a) escludere o limitare la responsabilità del professionista in caso di morte o danno alla persona del consumatore, risultante da un fatto o da un'omissione del professionista; b) escludere o limitare le azioni del consumatore nei confronti del professionista o di un'altra parte in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista; c) prevedere l'adesione del consumatore come estesa a clausole che non ha avuto, di fatto, la possibilità di conoscere prima della conclusione del contratto*".

Nelle differenti ipotesi di contratti "tra pari", ossia nei casi in cui il fruitore dei servizi di *cloud* non sia un consumatore, si applicherà la disciplina generale prevista dagli artt. 1341 e ss. del Codice Civile.

Secondo l'art. 1341 c.c. nei contratti standardizzati (condizioni generali di contratto) previsti per un numero indeterminato di rapporti e predisposti da uno dei contraenti, le clausole ivi contenute sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle utilizzando l'ordinaria diligenza[55]. Pertanto, secondo la disposizione normativa in commento il contraente, il fruitore dei servizi nel caso del *cloud computing*, deve sempre agire nella consapevolezza di quanto stabilito negli accordi contrattuali, anche in assenza di trattative.

Nel secondo comma dello stesso articolo il legislatore ha previsto l'inefficacia delle condizioni generali di contratto che stabiliscono uno squilibrio dei diritti e degli obblighi a favore di colui che le ha predisposte (il *cloud provider*, nei contratti del *cloud*), salvo che queste non siano state specificamente approvate per iscritto. Anche in questo caso, la norma, tutela la parte debole del contratto che, non avendo negoziato il contenuto dell'accordo, sarà comunque vincolato alle condizioni contrattuali già predisposte.

Proseguendo l'analisi dell'art. 1341 c.c., le clausole ritenute vessatorie sono quelle che stabiliscono limitazioni di responsabilità, facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze, limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi, tacita proroga o rin-

[55] L'ordinaria diligenza rappresenta la diligenza richiesta dall'uomo medio.

novazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria. Le ipotesi appena menzionate sono tassative e non sono suscettibili di interpretazione analogica.

Secondo la Giurisprudenza di legittimità, il termine "inefficacia" starebbe ad indicare un'ipotesi di nullità formale virtuale[56], ovvero una causa di nullità non espressamente prevista dalla legge come tale, ma così interpretata sulla scorta della natura imperativa delle norme che si intendono violate.

In virtù di questa interpretazione, le clausole vessatorie devono considerarsi nulle ai sensi dell'art. 1418 c.c. e quindi come non apposte al contratto. Inoltre, nel caso in cui le clausole vessatorie siano essenziali[57], ovvero qualora le parti, avendo conosciuto la nullità delle stesse, non avrebbero concluso il contratto, l'invalidità colpirebbe l'intero contratto.

Per evitare gli effetti dell'invalidità delle condizioni contrattuali vessatorie, il legislatore ha previsto che le parti debbano "*specificamente approvarle per iscritto*". Sul punto, un particolare orientamento giurisprudenziale sostiene che la sottoscrizione delle singole clausole deve avvenire "*utilizzando una tecnica di redazione che sia idonea a suscitare l'attenzione del sottoscrittore sul significato delle clausole specificamente approvate*"[58].

Sul punto, va rilevato che nei contratti del *cloud*, se conclusi con il mezzo delle tecnologie informatiche e telematiche, si ripresenta, come per tutti i contratti telematici, il problema della sottoscrizione delle singole clausole vessatorie. L'orientamento prevalente, sia in dottrina che in giurisprudenza, ritiene che anche nella contrattazione telematica, a tutela della parte debole del contratto, sia necessaria la sottoscrizione, seppure in forma elettronica, delle clausole. Nei contratti telematici, quindi, non è sufficiente il cd. "doppio *click*" o l'apposizione del segno di spunta accanto alle clausole contrattuali, bensì è richiesto una specifica approvazione per iscritto da parte di entrambe i contraenti.

Mentre nel documento cartaceo è agevole realizzare una doppia sottoscrizione, non può dirsi lo stesso per i contratti telematici. Per queste ragioni, le clausole vessatorie contenute nei contratti telematici devono ritenersi

[56] Cass. Civ., sez. III, 14 luglio 2009, n. 16394.

[57] L'essenzialità delle clausole deve essere valutata in riferimento all'intero accordo stabilito dalle parti.

[58] In tal senso si è espressa la Corte di Cassazione con la sent. 29 febbraio 2008, n. 5733.

tendenzialmente inefficaci ai sensi dell'art. 1341 c.c., a meno che queste non siano state oggetto di specifica approvazione mediante la loro riproduzione su un supporto cartaceo in accompagnamento al documento elettronico del contratto. Tuttavia, non può negarsi che tale soluzione rappresenti un notevole aggravio per i *cloud provider* e, più in generale, per l'intero mercato dei servizi in *cloud*.

Per ovviare a questa problematica, alcuni autori hanno proposto un'interpretazione evolutiva dell'art. 1341 c.c., in base alla quale sarebbe sufficiente il cd. "doppio *click*", purché l'aderente sia messo nella concreta possibilità di conoscere, senza confusione o modalità fuorvianti, il concreto contenuto delle condizioni generali di contratto[59].

Al di là delle proposte avanzate da più parti per realizzare la doppia sottoscrizione nei contratti conclusi nel *web*, la strada più certa e priva di incertezze interpretative, sarebbe quella della doppia apposizione della sottoscrizione digitale (firma digitale, qualificata o avanzata) nel modulo *online* o nel messaggio *e-mail* contenente le clausole vessatorie.

[59] Così BELISARIO E., "*Cloud Computing*" , *Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011, pag. 17 e ss. A sostegno dell'interpretazione in senso evolutivo, l'Autore ritiene che la specifica approvazione per iscritto è richiesta dal legislatore del 1942 che all'epoca conosceva poche modalità di conclusione del contratto tra le quali quella indubbiamente prevalente era la forma scritta. Inoltre, la finalità della "specifica approvazione per iscritto" segue la logica di consentire al contraente di valutare e ponderare circa la possibilità di concludere un contratto contenente pattuizioni per lo stesso particolarmente onerose. Detta finalità, oggi, può essere ampiamente soddisfatta con il cd. "doppio *click*".

PARTE SESTA - ECCELLENZE E CASI DI STUDIO

1. Le prime eccellenze Cloud nella sanità pubblica e privata

La Pubblica Amministrazione sanitaria è caratterizzata da una netta separazione delle funzioni e delle specialità in ambito clinico-medico e da un modello gestionale di tipo aziendale. Con l'avvento del Fascicolo Sanitario Elettronico ("*Electronic Health Record*" – EHR[1]), tra i più significativi strumenti di digitalizzazione della sanità, le singole strutture sanitarie oggi sono in grado di cooperare tra loro nell'ambito di un modello organizzativo divenuto oramai multidisciplinare, valorizzando l'integrazione dei professionisti e migliorando i processi di cura dei pazienti.

La complessa organizzazione del Sistema Sanitario Nazionale (SSN) è in continua e rapida evoluzione. L'introduzione di nuove realtà territoriali, quali ASL, Aree Vaste, strutture regionali, provinciali e locali (e non solo), ha reso sempre più complesso il coinvolgimento di tutti gli interessati e, di conseguenza, la capacità di operare in modo integrato da parte dei sistemi informativi di ciascuna.

Per far fronte a queste problematiche, già a partire dal 1998, negli Stati Uniti, è stato elaborato un progetto di integrazione dei sistemi informativi sanitari, poi importato anche in Europa, al fine di facilitare il dialogo tra varie strutture e, quindi, di migliorarne le prestazioni a favore dell'utente-paziente. L'iniziativa prende il nome di "*Integrating the Healthcare Enterprise*" – IHE[2]; con essa si promuove l'adozione coordinata di *standard* consolidati attraverso la creazione e la manutenzione di documenti tecnici, per garantire la comunicazione e lo scambio di informazioni tra diverse strutture cliniche.

---

[1] G. ARMELLIN, D. BETTI, F. CASATI, A. CHIASERA, G. MARTINEZ, J. STEVOVIC, *Privacy preserving event driven integration for interoperating social and health systems*, Secure Data Management: 7th Vldb Workshop (SDM'10), September 2010.

[2] J. ERICSON, *Health intelligence: An End to "Needless"*, Information Mangement, February 2012.

Non vi è dubbio, quindi, che l'introduzione del Fascicolo Sanitario Elettronico (FSE) rappresenti uno strumento di grande utilità per favorire il processo di integrazione delle informazioni, rappresentando esso stesso un mezzo di condivisione ed elaborazione dei dati clinici di un paziente[3].

Il FSE, così come definito all'art. 12 del d.l. 18 ottobre 2012, n. 179, rappresenta l'insieme dei dati e dei documenti digitali attraverso i quali è possibile ricostruire l'intera storia clinica del singolo paziente. Esso non va confuso con gli altri strumenti di gestione informatizzata quali la Cartella clinica elettronica, il Dossier Sanitario e il Referto online, già esaminati nel capitolo precedente.

I mutamenti intercorsi nell'ambito della sanità fanno parte del complicato processo di progressiva informatizzazione di tutti gli aspetti e le dimensioni sociali. Tutte le attività umane sono orientate verso una continua evoluzione che contempla l'utilizzo sempre più diffuso di nuove apparecchiature e tecnologie in grado di interconnettere diversi apparati informativi e condividere informazioni (Figura 17).

Figura 17: Esempi di nuove tecnologie[4]

Alla luce di quanto affermato si può osservare quanto la rivoluzione tecnologica abbia cambiato le esigenze dei cittadini, favorendo l'aumento della consapevolezza degli utenti rispetto alle problematiche sociali e politiche,

[3] Come si è visto, il FSE è costituito dalla raccolta di tutti i dati clinico-sanitari acquisiti nell'arco dell'intero ciclo di vita di un individuo, con lo scopo di supportare la continuità di cura, l'educazione e la ricerca.

[4] Fonte: *Cloud Computing in sanità Un nuovo paradigma di sviluppo*, Gruppo24Ore, 2012, p. 96.

comprese quelle inerenti il settore sanitario. Non si può negare come, attualmente, tutti i cittadini siano maggiormente attenti alla qualità dei servizi e dell'assistenza offerta dal SSN, aumentando il livello delle richieste di servizi sempre più evoluti.

Nello scenario attuale, quindi, il sistema sanitario deve far fronte a nuove esigenze in conseguenza delle mutate dinamiche sociali, innovando i sistemi di IT della sanità sia pubblica che privata. In particolare, è necessario implementare ambienti distribuiti ed eterogenei, garantire la scalabilità e la dinamicità delle risorse e, nello stesso tempo, fornire capacità e performance adeguate alle nuove sfide, garantendo la sicurezza dei dati e il controllo degli accessi.

Affinché avvenga effettivamente questa evoluzione, è necessario che il mondo delle imprese e dei professionisti del settore siano disposti ad investire notevoli risorse per la realizzazione di soluzioni clinico sanitarie innovative ed economicamente sostenibili, garantendo allo stesso modo adeguati livelli di prestazioni, di sicurezza e di integrabilità verso sistemi sempre più distribuiti ed interconnessi.

A conclusione del percorso, fin qui condotto, questa sesta e ultima parte sarà dedicata all'illustrazione di alcuni casi pratici di applicazioni *cloud computing* al settore sanitario. I primi rappresentano una breve panoramica dei casi di eccellenza presentati in occasione di vari convegni pubblici. Seguirà l'illustrazione più dettagliata di due casi di studio: "Vitaever" ed "eTriage".

1.1 Caso n. 1 - Azienda per i Servizi Sanitari n.4 Medio Friuli

L'Azienda per i Servizi Sanitari n° 4 Medio Friuli, oggi Friuli Centrale, fornisce i propri servizi sanitari a circa 350.000 cittadini distribuiti su una superficie di 1.807 Km quadrati. La propria struttura si articola in 5 distretti sanitari (Cividale, Codroipo, San Daniele, Tarcento e Udine), in 3 dipartimenti territoriali di Salute Mentale, Dipendenze e Prevenzione e comprende l'ospedale di San Daniele del Friuli e l'Istituto di Medicina Fisica Riabilitativa Gervasutta di Udine.

A partire dal 2010 l'Azienda sanitaria Medio Friuli ha avviato un progetto finalizzato ad assegnare a tutti i 320 medici di medicina generale e ai pediatri di libera scelta, attivi sul proprio territorio di competenza, una casella di posta elettronica con un unico dominio, con l'obiettivo di agevolare le comunicazioni con le altre strutture sanitarie operanti negli altri cinque distretti regionali.

Trascorsi pochi mesi dall'attivazione del progetto, circa il 70% dei medici coinvolti ha attivato la propria casella di posta elettronica sotto il dominio unico Gmail. Grazie a questo progetto è stato possibile condividere informazioni e aggiornamenti (dai protocolli interni alle indicazioni sulle certificazioni INPS e così via) in modo rapido ed efficace attraverso la creazione di un'unica mailing list comprensiva di tutti i medici dell'Azienda.

Nell'ambito di un solo distretto è stato sperimentato l'uso del servizio Google Sites per la creazione di un sito *web* nel quale tutti gli operatori sanitari potessero consultare tutti i documenti attraverso l'uso dell'algoritmo di ricerca Google. L'obiettivo è quello di coinvolgere non solo tutti gli altri distretti dell'Azienda sanitaria, ma anche quello di consentire la condivisione di informazioni con le associazioni di volontariato e altri enti. La scelta consente un notevole risparmio economico grazie alla possibilità di sviuppare e creare mini portali *web*, leggeri, direttamente aggiornabili da parte dei singoli produttori dei contenuti e fruibili all'esterno, senza dover necessariamente ampliare le sezioni del sito web ufficiale.

Infine, nella seconda fase, con il progetto Google Apps sono state estese le soluzioni di comunicazione Google a tutti i 2.500 addetti dell'Azienda sanitaria, in sostituzione dei precedenti protocolli basati su Send Mail ed Exchange.

Grazie ai servizi attivati, attualmente tutto il personale dell'Azienda sanitaria friulana può accedere, da qualunque luogo e con qualsiasi dispositivo, alla posta elettronica e alle informazioni contenute nei documenti condivisi sui siti Google Sites.

Inoltre, tutto il personale medico ha a disposizione un archivo di informazioni sempre aggiornato e facilmente accessibile. La semplicità di implementazione e di utilizzo delle soluzioni tecnologiche ha consentito una rapida diffusione dell'applicazione a costi molto contenuti, non essendo stato necessario il ricorso ad un supporto del personale tecnico. Eventuali

problemi o difficoltà di utilizzo trovano ampie risposte nei servizi gratuiti di *help online* di Google.

Il passaggio a Google Apps è stato dettato principalmente dall'esigenza di eliminare i vecchi sistemi di gestione delle comunicazioni, divenuti ormai obsoleti e dai costi fissi elevati, essendo gestiti in-house da risorse esterne.

L'esperienza rappresenta una valida soluzione per introdurre notevoli risparmi, derivanti dall'abbattimento dei costi per la gestione e per il personale specializzato interno, in un settore come quello della posta elettronica che, pur essendo un servizio fondamentale per le attività, non costituisce il *core* di un'azienda sanitaria.

1.2 Caso n. 2 - Azienda Ospedaliero-Universitaria Udine

L'Azienda Ospedaliero-Universitaria (A.O.U.) di S. Maria della Misericordia di Udine, sorta nel 2006 in seguito alla fusione del Policlinico Universitario con l'Azienda Ospedaliera S. Maria Della Misericordia, si articola in tre Poli ospedalieri: Udine, Cividale del Friuli e Gemona del Friuli.

Presso l'A.O.U. sono impiegati oltre 4.000 dipendenti e collaboratori per un totale di mille posti letto disponibili. Ogni giorno oltre 6.000 persone accedono alle strutture, di cui 237 si avvalgono dei servizi di Pronto Soccorso e, complessivamente, vengono erogate 2.813 visite ed esami strumentali.

Nel 2010 l'A.O.U., in collaborazione con NB Factory, partner CISCO, ha attivato un progetto finalizzato all'attuazione di interventi strutturali a tutela della sicurezza informatica aziendale, previsti dal Piano Attuativo Ospedaliero 2010. Con il progetto l'Azienda Ospedaliera ha inteso migliorare la propria infrastruttura informatica con l'introduzione della tecnologia VoIP e con l'adozione di sistemi dedicati all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali. (cosiddetti PACS - *Picture archiving and communication system*).

Nella prima fase del progetto è stato ampliato il parco macchine dell'Azienda Ospedaliera, composto da circa 100 *server* fisici, 80 armadi

tecnologici, 200 apparati di rete attivi, per un totale di 2.200 postazioni di lavoro, di cui circa 300 sostituite ogni anno e circa 200 acquisite *ex novo*.

In seguito è stata realizzata una nuova sala server, in aggiunta a quella già esistente, ed è stato implementato il *Network Admission Control* (NAC), un sistema per la verifica delle *policy* di sicurezza di tutte le risorse di rete; in questo modo, in attuazione delle *policy* di sicurezza informatica definite dalla Funzione IT, è stato possibile consentire l'accesso solamente ai dispositivi ritenuti conformi e affidabili.

Infine, con la tecnologia della virtualizzazione l'Azienda Ospedaliera ha razionalizzato il proprio parco *server*, concentrando nel nuovo *data center* le diverse macchine prima dislocate nelle varie sedi, aumentando l'efficienza nella gestione delle risorse informatiche aziendali.

Attualmente sono presenti circa 100 *server* virtuali installati su *hardware* CISCO UCS Blade e macchine *storage* in configurazione *metrocluster* connesse ad un centro stella con *switch* Cisco Catalyst 6500.

Il progetto prevede altresì la virtualizzazione dei *desktop* aziendali, consentendo così la separazione dell'ambiente *desktop* dalle postazioni fisiche, sfruttando i benefici di un'architettura *client-server*. Grazie ai *desktop* virtuali ospitati nei server centrali, qualunque operatore può lavorare sul proprio PC *client* accedendo tramite proprio ID alla rete aziendale, alle applicazioni e ai dati, sfruttando la capacità di calcolo dei *server*.

Grazie alla nuova architettura IT è stato possibile rinnovare l'intero sistema informativo aziendale, migliorando sia i processi decisionali sia i processi clinici.

L'infrastruttura garantisce maggiore efficienza nella gestione e nel controllo delle risorse di rete e, allo stesso tempo, la sicurezza delle informazioni e dei dati sanitari dei pazienti.

Inoltre, il progetto ha consentito la semplificazione dell'infrastruttura IT e la gestione automatica delle procedure di *backup*, riducendo la richiesta di attività di manutenzione e migliorando la continuità operativa nell'erogazione dei servizi IT.

Infine, grazie alle soluzioni di *cloud computing* adottate, l'Azienda Ospedaliera sarà in grado di erogare i propri servizi ad altre strutture sanitarie locali, ammortizzando così i costi affrontati per la realizzazione dell'infrastruttura.

1.3 Caso n. 3 – Ente Mutuo Milano

L'Ente Mutuo di assistenza tra gli Esercenti il Commercio della Provincia di Milano è stato costituito nel 1955 nell'ambito dell'Unione Commercianti; in particolare, l'Ente Mutuo è un'Associazione di Mutua Assistenza senza scopo di lucro avente per oggetto l'assistenza sanitaria dei propri iscritti. Attualmente è composta da circa 25 mila soci, per ciascuno dei quali sono iscritti anche i componenti del nucleo familiare in qualità di soci beneficiari. Tra le prime forme di assistenza sanitaria integrativa a livello nazionale, l'Ente Mutuo si rivolge esclusivamente agli Imprenditori ed ai Professionisti iscritti alle Associazioni aderenti ad Unione Confcommercio Imprese per l'Italia Milano - Lodi - Monza e Brianza. Le strutture convenzionate sono oltre 680 e comprendono Studi Medici, Poliambulatori, Laboratori di Analisi, Ospedali e Cliniche Private in grado di erogare assistenza ospedaliera e ambulatoriale nel rispetto dei requisiti previsti dalla normativa regionale.

Nel 2010 l'Ente Mutuo di assistenza ha attivato un progetto finalizzato alla creazione di un sistema informatico integrato in grado di gestire tutti i processi aziendali. Il sistema è progettato in *cloud* privato e consente l'accesso a circa cento utenti, sia interni che esterni all'azienda, compresi gli operatori sanitari delle case di cura, degli studi medici e delle altre strutture convenzionate. Il progetto è realizzato grazie ai servizi di Axioma, *business partner* di IBM, tramite la soluzione OnlyConnect, uno strumento di *Enterprise Communication* e *Collaboration* in grado di supportare le relazioni con i vari soggetti coinvolti nei rapporti aziendali. Attraverso un unico *database* tutte le informazioni (*email* aziendali, documenti, contatti, appuntamenti) sono gestite e correlate tra loro, per consentire a tutti gli utenti una gestione pratica e corretta di ciascuna relazione.

Prima dell'attivazione del progetto le procedure erano gestite in parte manualmente mediante l'uso di singoli applicativi, con tutte le inefficienze derivanti. Attualmente, il nuovo sistema integrato consente la gestione degli assistiti attraverso le schede anagrafiche e le posizioni contributive, permette di gestire le impegnative per le prestazioni sanitarie erogate, i rimborsi dei soci e le convenzioni con le strutture sanitarie. Sotto il profilo

amministrativo, il sistema consente di gestire i rapporti con le banche, la contabilità e il *marketing*.

Per ovvie ragioni, considerata la natura e la delicatezza dei dati trattati con i nuovi sistemi, sono stati adottati tutti gli accorgimenti necessari per garantire un elevato standard di sicurezza; questi aspetti sono interamente gestiti dall'Azienda partner che fornisce anche servizi di assistenza e manutenzione.

I primi benefici ottenuti con l'adozione del sistema in *cloud* sono rappresentati da un aumento dell'efficienza e della velocità dei processi gestionali, prima caratterizzati dalla presenza di errori, rallentamenti e, talvolta, perdita dei dati. Altri effetti positivi sono rappresentati dalla riduzione dei tempi di gestione dell'iter burocratico di alcune pratiche interne e, conseguentemente, dalla possibilità di dedicare più tempo e risorse ad attività a maggiore valore aggiunto. Infine, anche il settore *marketing* e vendite ha ottenuto numerosi benefici, considerata l'elevata complessità del sistema delle vendite, della rete di agenti nel territorio e del recupero crediti.

1.4 Caso n. 4 – BrainCare

Fondata nel 2010, BrainCare riunisce medici, psicologi, psicoterapeuti e tecnici informatici impegnati a realizzare nuove modalità di approccio al benessere psicofisico e alla salute delle persone. In particolare, BrainCare lavora nel settore della riabilitazione dell'individuo affetto da disturbi cognitivi conseguenti a disfunzioni cerebrali, si occupa di valutazione del potenziale delle risorse umane, anche attraverso *bio feedback*, e di formazione e ricerca medica in cooperazione con strutture ospedaliere, medici di medicina generale, ASL e università. Attualmente BrainCare è presente in Italia con quattro centri operativi di proprietà (BrainCare Clinic Point) a Padova, Ferrara, Bologna e Rovigo. La struttura è predisposta anche per l'apertura di centri affiliati in *franchising*.

1.4.1 L'applicazione: *cloud computing* per un *network* in *franchising*

La strategia di business di BrainCare prevede lo sviluppo di una rete di centri clinici affiliati in tutta Europa e, per la sua realizzazione, richiede

l'uso di strumenti informatici per la gestione delle attività e dei contatti con la casa madre. Per realizzare ciò, tutti i centri clinici sono collegati alla rete dati di BrainCare e le telecomunicazioni aziendali sono relizzate attraverso la tecnologia VoIP. In collaborazione con Eniac è stato sviluppato un sistema informativo sul modello del *cloud computing* per la gestione del *network* dei centri affiliati. Il primo step è consistito nella realizzazione della piattaforma applicativa *web* Tener-a-mente 2.0 che integra al proprio interno diversi applicativi: dal sistema ERP (*Enterprise resource planning*) che integra tutti i processi relativi all'amministrazione e alla finanza dell'intera struttura, ai sistemi per la gestione dell'operatività dei centri clinici.

Tramite i *software* in dotazione, ciascun collaboratore di BrainCare appartenente ai vari centri può condividere le proprie agende, calendari e documenti, può accedere al Manuale della Qualità aziendale e alla documentazione relativa ai processi e alle procedure standard da adottarsi in ciascun centro.

Grazie ad un sistema CRM (*Customer Relationship Management*) ciascun centro può gestire le relazioni con i propri clienti, organizzando le schede cliniche dei pazienti, tracciando i profili e la documentazione personale che viene poi raccolta e conservata in un sistema di gestione documentale. Inoltre, gli applicativi in uso per la raccolta dei risultati degli esami medici e l'elaborazione delle misurazioni effettuate sono interfacciati con il sistema CRM.

Per realizzare i propri obiettivi di espansione verso altri mercati con la formula del franchising, BrainCare necessita di erogare servizi IT ai propri centri affiliati. A tal fine è stato utilizzato un modello di *cloud computing* in cui i sistemi informativi aziendali sono ospitati presso il data center di un *provider hosting* così da consentire a BrainCare di richiedere al *provider* il potenziamento delle risorse dedicate al sistema Tener-a-mente 2.0, in proporzione alle dinamiche di crescita del *business* aziendale. I centri clinici, quindi, accedono da remoto ai sistemi informativi nel pieno rispetto dei criteri di continuità operativa e di sicurezza, garantiti grazie alla sottoscrizione di accordi di *Service Level Agreement* (SLA) con il *provider*.

L'adozione di soluzioni *cloud computing* consente di supportare facilmente lo sviluppo di un vero e proprio *network* di nuovi centri clinici periferici. Infatti, le tecnologie adottate consentono di realizzare in poco

tempo lo *start up* dei nuovi centri, attivando i vari servizi IT e allocando le risorse necessarie. Con questo sistema, BrainCare non necessita di dotarsi di un proprio *data center* centrale, né di personale specializzato e dedicato alla loro gestione, con un evidente e notevole risparmio di costi.

Inoltre, la continuità operativa dei servizi IT, la sicurezza dei dati sensibili, l'aggiornamento applicativo sono garantiti interamente dai *partner* tecnologici di BrainCare, che non deve occuparsi degli aspetti legati alla loro gestione.

Infine, la centralizzazione del sistema informativo consente, da una parte, un maggiore controllo dei centri sia sotto l'aspetto clinico che sulle risorse e, dall'altra, la garanzia che in ogni struttura siano adottate le medesime norme, procedure e processi codificati e che la gestione di tali attività sia garantita integralmente dal centro.

1.5 Caso n. 5 – Azienda Ospedaliera di Desio e Vimercate

Nata nel 1998, l'Azienda Ospedaliera di Desio e Vimercate, nel gennaio 2009 ha assunto l'attuale struttura e denominazione in seguito alla riorganizzazione del sistema sanitario lombardo e all'istituzione della Provincia di Monza e Brianza (D.c.r 19 marzo 2008 n. VII/579). Attualmente l'Azienda si articola in 5 presidi ospedalieri (Carate Brianza, Desio, Giussano, Seregno, e Vimercate) e 11 strutture sanitarie territoriali (poliambulatori) per un totale di circa 3.100 dipendenti e oltre 1.200 posti letto per ricoverati. Ogni anno vengono eseguiti circa 60 mila ricoveri, pari a 320 mila giornate di degenza, e vengono erogate circa 6 milioni di visite ambulatoriali specialistiche.

L'Azienda Ospedaliera di Desio e Vimercate ha inteso procedere alla dematerializzazione della documentazione clinica, attraverso la digitalizzazione dei referti, delle immagini radiologiche e della cartella clinica dei pazienti. A supporto della digitalizzazione è stato necessario attivare dei servizi per la conservazione a norma di legge della documentazione digitale e, allo stesso tempo, un servizio per la gestione e il supporto dell'intera attività ospedaliera. Per rispondere a queste esigenze, in collaborazione con NETAPP e VEM sistemi, è stato attivato un progetto di

rinnovamento tecnologico dell'infrastruttura informatica aziendale mediante tecnologie di virtualizzazione in grado di razionalizzare, centralizzare e ottimizzare l'infrastruttura IT.

In precedenza, l'infrastruttura era costituita da tre data center dislocati nei tre principali presidi ospedalieri: Vimercate (60 *server* fisici), Desio (30 *server* fisici) e Carate Brianza (10 *server* fisici). Presso ogni *data center* era predisposta una *Storage Area Network* (SAN) per l'erogazione dei servizi applicativi e l'acceso ai dati locali.

La nuova infrastruttura è stata realizzata per rispondere a due distinte esigenze: da una parte, ottenere il consolidamento della struttura *hardware* e, dall'altra, assicurare una maggiore continuità di servizio e sicurezza dei dati.

Attualmente la struttura IT si compone di due *data center* "gemelli" ubicati nel presidio ospedaliero di Vimercate all'interno di due strutture fisiche distinte e collegate mediante la fibra ottica. Nelle strutture sono ospitati circa 30 *server* fisici, per un totale di 300 macchine virtuali, e un sistema di archiviazione dati con scrittura sincrona. Il nuovo sistema è in grado di garantire la continuità operativa anche in caso di indisponibilità o malfunzionamenti totali o parziali di una delle due strutture "gemelle". Il *backup* è garantito in tempo reale grazie all'installazione di una SAN aggiuntiva collocata in un presidio ospedaliero diverso, dedicata esclusivamente alle copie di sicurezza.

La razionalizzazione e la riallocazione su *server* virtuali, oltre a semplificare l'uso e migliorare le prestazioni, ha consentito di aumentare il livello di affidabilità dei sistemi e di garantire la *Business Continuity* ed il *Disaster Recovery*. In generale, la semplificazione della struttura e l'automatizzazione del *backup* hanno consentito un risparmio economico dovuto alla razionalizzazione delle attività di manutenzione.

La nuova infrastruttura IT ha garantito maggiore flessibilità di gestione delle risorse e l'affidabilità dei sistemi grazie alla continuità operativa. Inoltre, grazie alla riduzione del numero dei *server fisici* e alla scalabilità dei sistemi, è stato possibile investire in nuovo *hardware*, grazie ai risparmi ottenuti con la riduzione dei costi di manutenzione.

La virtualizzazione dell'infrastruttura IT consente all'Azienda Ospedaliera di aumentare il livello di sicurezza fisica e informatica

dell'intera rete e di beneficiare di un sistema di continuità operativa anche in caso di indisponibilità totale di uno dei *data center*.

La nuova infrastruttura, realizzando di fatto una soluzione di *business continuity* con *disaster recovery*, è in grado di supportare tutta l'attività ospedaliera che, in seguito alla digitalizzazione, richiede un livello di servizio 24/7; infatti, una qualunque interruzione o malfunzionamento potrebbe generare conseguenze negative ai cittadini stessi, non solo in termini di disservizi.

L'infrastruttura consente ad oltre 500 medici e 1.600 infermieri di gestire, ogni giorno, i dati clinici di circa 800 pazienti (inquadramento clinico medico ed infermieristico, prescrizioni, somministrazioni di terapie, pianificazione e rilevazione di parametri vitali e di bisogni assistenziali). Infine, con la nuova infrastruttura IT l'Azienda Ospedaliera è in grado di pianificare l'evoluzione dei propri servizi e di offrire gli stessi ad altre aziende ospedaliere sul modello di un *cloud* privato interaziendale.

1.6 Caso n. 6 – Clinica Dentale s.r.l

Clinica Dentale s.r.l. è stata fondata nel 2007 da tre soci e ha sede presso Grancona (VI) e Torri di Quartesolo (VI). Clinica Dentale è una società certificata ISO 9001 che offre un'ampia gamma di servizi: Prevenzione Igiene orale, Conservativa, Endodonzia, Implantologia, Ortodonzia, Protesi, Parodontologia, Pedodonzia, Gnatologia Ortopedia e Osteopatia, Medicina Estetica e diversi corsi di aggiornamento.

La struttura di Grancona dispone di 7 sale operative, mentre la sede di Torri di Quartesolo, inaugurata nel marzo del 2010, è dotata di 36 sale operative. In collaborazione con Redder, Clinica Dentale ha realizzato una rete di fonia e dati in grado di centralizzare i servizi di telefonia e migliorare l'accesso ad *internet*, al fine di garantire una più efficiente comunicazione tra le due sedi e supportare l'attività svolta nelle varie sale operative.

L'obiettivo della nuova infrastruttura IT è di garantire la disponibilità dei dati in entrambe le sedi e nelle 43 sale operative, l'accesso alle cartelle cliniche dei pazienti e alle agende di lavoro dei vari operatori sanitari, a supporto dell'attività operativa e amministrativa dell'azienda.

L’architettura IT prevede un Centro Elaborazione Dati (CED) presso la sede di Torri di Quartesolo, un *server* IBM X3650 in alta affidabilità con VMware Vsphere 4.1, una SAN in fibra DS4700 per il sito primario, e una SAN DS3400 per il sito secondario di *disaster recovery*.

Prima della realizzazione della nuova infrastruttura, le sedi aziendali erano collegate tramite VPN (*Virtual Private Network*); tuttavia, l’inaffidabilità della connettività, l’interruzione delle chiamate interne, le difficoltà di collegamento ai dati e i frequenti riavvii dei sistemi diagnostici causavano non pochi disservizi nella gestione del paziente, con conseguenti perdite economiche notevoli.

Il nuovo progetto ha previsto un collegamento ad *internet* ad alta affidabilità per ogni sede della clinica affiancando alla connettività principale una di *backup*; quest’ultima, attivata istantaneamente, garantisce la continuità della connessione e dell’operatività, evitando ogni interruzione.

Le due forme di connettività sono garantite grazie a due diverse tecnologie e il passaggio da una all’altra avviene immediatamente in modo automatico così che, quando la connettività principale si interrompe, tutti i dati passano nella connessione secondaria e arrivano a destinazione senza evidenziare il malfunzionamento.

La continua disponibilità di connettività consente la condivisione, in modo rapido e sicuro, delle immagini diagnostiche ad alta definizione. Inoltre, è stato realizzato un canale VoIP dedicato ed è stata riservata un’apposita banda per la radio *in-store*. Le linee voce sono state converite in *VoIP*, fatte convergere verso un’unica sede e gestite da un *call center* centralizzato in grado di smistare le chiamate. L‘implementazione di fax virtuali ha consentito a tutto il personale di gestire, inviare e ricevere le comunicazioni via fax direttamente dalle proprie postazioni informatiche. Infine, la creazione di un *hotspot* gratuito per i clienti permette agli stessi di scaricare dati dalla rete senza interferire sull’operatività dell’azienda.

Tutta la struttura, la sicurezza dell’*hotspot*, l’autenticazione e il tracciamento delle sessioni sono gestite in *cloud* dal *partner* Redder.

Grazie alla nuova infrastruttura di rete, le due sedi della Clinica Dentale s.r.l. possono comunicare in modo rapido e diretto, senza patire alcuna interruzione dei servizi. Il miglioramento della connettività ha reso più efficiente la gestione dell’attività della clinica, delle prenotazioni delle

visite, delle schede dei pazienti e la condivisione delle immagini diagnostiche. Infine, con la nuova infrastruttura Clinica Dentale ha raggiunto la continuità operativa e un incremento del *business*, grazie anche ai risparmi ottenuti con l'adozione del *VoIP*.

1.7 Caso n. 7 – La piattaforma X1V1della *suite* ADPERSONAM

La piattaforma X1V1 della *suite* ADPERSONAM, prodotta da Dedalus S.p.a., nella sua prima versione nasce nel 1996. In seguito si è notevolmente evoluta fino a divenire uno degli strumenti più avanzati per l'applicazione di modelli innovativi di assistenza sanitaria. Attualmente la piattaforma è conforme ai requisiti richiesti dai principali *standard* internazionali (IHE, HL7[5], HSSP[6]), è scalabile e si compone di diversi moduli con oltre 20 componenti specializzati.

Il sistema X1V1 permette alle Amministrazioni sanitarie di implementare un *Electronic Medical Record* (EMR)[7], un *Electronic Patient Record* (EPR)[8] di livello aziendale e, soprattutto, un *Electronic Health Record* (EHR)[9]. Inoltre, con i sistemi di Dedalus è possibile interfacciarsi con tutte le informazioni e i dati clinico/sanitari dei pazienti e fornire una serie di servizi per il cittadino, tra cui l'accesso ai documenti elettronici firmati digitalmente dai professionisti operanti nel settore sanitario. Infine, la piattaforma

[5] *Talend: Cloud Enabled Open Source Integration Software*, http://www.talend.com/products-talend-cloud/.

[6] *TC3 Health Case Study: Amazon Web Services*, http://aws.amazon.com/solutions/case-studies/tc3-health/.

[7] L'espressione "*Electronic Medical Record*", maggiormente utilizzata nei Paesi americani e asiatici, indica la raccolta di informazioni relative ad un particolare settore della medicina (es. cardiologia, chirurgia, neurologia, ecc.). Il EMR è sviluppato nell'ambito di una struttura sanitaria e può essere condiviso con altri settori appartenenti alla medesima struttura.

[8] Secondo una definizione elaborata dal Servizio sanitario nazionale inglese, l'espressione "*Electronic Patient Record*" indica una raccolta di informazioni relative a singoli interventi di cura di un paziente, appartenenti principalmente ad una singola struttura.

[9] L'*Internatonal Standard Organisation* (ISO) ha definito "*Electronic Health Record*" come una raccolta di informazioni in formato elettronico riguardanti la salute di un paziente.

consente la raccolta di informazioni "*cross-enterprise*" e degli operatori della sanità.

L'architettura è di tipo modulare (Figura 18), pertanto si adatta facilmente alle diverse esigenze delle molteplici realtà delle strutture sanitarie, fino ad arrivare ai singoli medici di famiglia, ai medici pediatri e ai singoli pazienti.

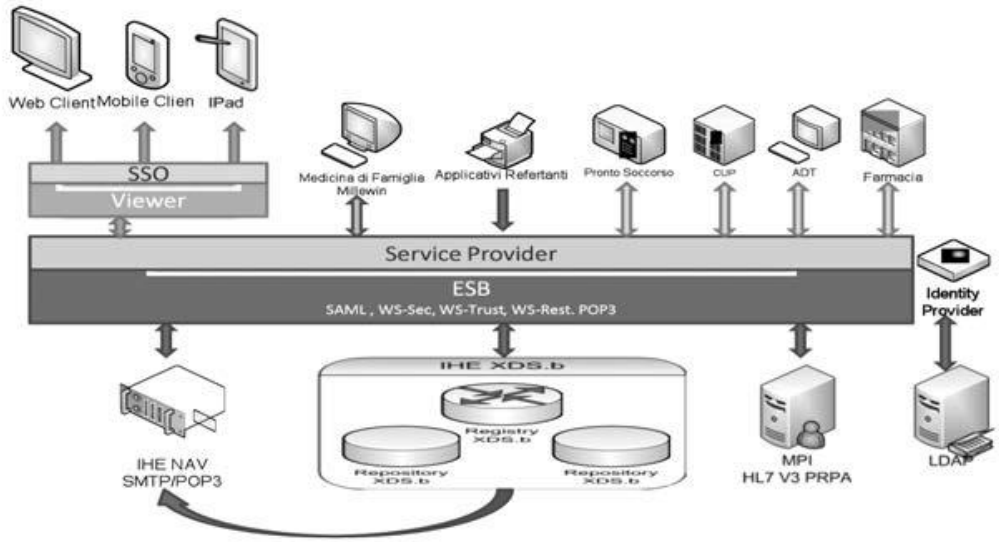

Figura 18: Architettura della piattaforma X1V1[10]

Con la piattaforma X1V1 è stato adottato un modello *cloud* di tipo *as a Service* affinché le risorse necessarie all'uso della piattaforma potessero essere configurate rapidamente in funzione dei moduli da attivare o delle specifiche esigenze della struttura sanitaria.

Nell'ambito di un progetto cofinanziato dall'Unione Europea e con l'intervento di partner internazionali, la piattaforma si è evoluta in un modello *Cloud-based* basato sullo standard SoA (*Service oriented Architecture*) e sarà testabile automaticamente tramite *framework* di test standardizzati.

[10] Fonte: *Cloud Computing in sanità Un nuovo paradigma di sviluppo*, Gruppo24Ore, 2012, p. 99.

2. Il progetto Vitaever

Vitaever è un progetto che nasce con l'obiettivo di fornire un supporto tecnologico alle attività di Assistenza Domiciliare Integrata (ADI), il servizio che permette ai cittadini che ne hanno bisogno di essere assistiti presso la propria abitazione attraverso dei programmi personalizzati, evitando così il ricovero presso strutture ospedaliere o case di riposo, per un tempo maggiore del necessario.

Il servizio Vitaever[11] è stato sviluppato da Nethical s.r.l., un'azienda IT bolognese che da oltre 10 anni si occupa di supportare, con la tecnologia e l'innovazione, le organizzazioni che svolgono attività di assistenza domiciliare e territoriale.

Grazie alla piattaforma della Nethical s.r.l. è possibile gestire un elevato numero di dati clinici (diagnosi, problematiche, cartelle cliniche, sintomi, e così via) e, nel contempo, migliorare il coordinamento di tutte le figure professionali coinvolte nell'erogazione di servizi sanitari.

A partire dal 2011, anno in cui Vitaever è stata lanciata sul mercato, sono state erogate oltre sei milioni di prestazioni sanitarie, per un totale di più di 20.000 assistiti. Attualmente, più di 1.300 operatori su tutto il territorio nazionale utilizzano Vitaever per gestire oltre 14.000 assistiti.

2.1 Caratteristiche

Tra le principali funzionalità, Vitaever consente la creazione di agende personalizzate per ogni Operatore coinvolto nel processo di cura del paziente, un sistema di geolocalizzazione in grado di calcolare il percorso migliore per raggiungere l'assistito e la gestione di tutti i dati e le informazioni cliniche delle attività svolte. Inoltre, sono state implementate diverse funzionalità amministrative in grado di semplificare la gestione della fatturazione e della rendicontazione delle attività svolte, tenendo traccia delle apparecchiature, dei presidi, dei farmaci e dei pasti consegnati presso il domicilio degli assistiti. Il servizio di reportistica, anche in forma grafica, permette di monitora-

[11] Per una lettura più dettagliata del progetto, delle sue caratteristiche e funzionalità si rimanda alle pagine presenti sul sito web ufficiale raggiungibile all'indirizzo http://www.vitaever.com/

re e valutare le attività degli operatori, le risorse utilizzate e i costi delle attività stesse, migliorando e facilitando la gestione globale.

Ciascun modulo funzionale di Vitaever è accessibile dagli utenti a seconda del profilo e dei permessi ad esso associati; ogni modulo può essere attivato e disattivato in base alle esigenze e sulla base del gruppo di appartenenza.

La piattaforma Vitaever è in grado di gestire le anagrafiche complete degli assistiti, degli operatori e degli utenti. Ogni assistito può essere assegnato a ciascun reparto della struttura e ogni operatore può lavorare su più reparti, attraverso diverse tipologie di azioni consentite a seconda del tipo di profilo o gruppo di appartenenza. La modalità di gestione implementata consente all'amministratore di sistema il pieno controllo degli accessi alle risorse. Inoltre, il sistema prevede procedure di importazione ed esportazione per garantire l'interoperabilità con altri *software*.

Di seguito si illustrano, brevemente, le principali funzionalità del sistema Vitaever.

Gestione anagrafiche, assistenze e programmazione attività

Ogni assistito è associato ad una specifica assistenza, ovvero il periodo all'interno del quale gli operatori possono svolgere attività sugli assistiti. Per ciascun periodo di assistenza è associabile una moltitudine di dati differenti (livello delle cure, ASL, distretto di riferimento, e così via) consentendo, quindi, di definire dettagliatamente la storia clinica di ciascun paziente. Infine, la gestione delle assistenze consente una precisa rendicontazione e analisi dei dati raccolti.

Con Vitaever è possibile gestire la programmazione delle attività, grazie alla presenza di una agenda personale per ogni operatore. Quest'ultimo, mediante un'interfaccia semplice e intuitiva, può organizzare e gestire differenti attività, anche mediante accesso da dispositivi *mobile*. L'agenda consente di organizzare gli appuntamenti esterni, ovvero le attività rivolte agli assistiti (es. consegna dei presidi, visite mediche, colloqui con i familiari), appuntamenti esterni (es. stesura di diari, colloqui formazione, coordinamento) e, infine, appuntamenti di gruppo, ovvero attività che coinvolgono gruppi di assistiti (es. consegna farmaci). Infine, è possibile gestire gli appuntamenti impostando la ripetizione delle attività, oppure visualizzando gli appuntamenti

di ciascun assistito rendendo agevole la sostituzione dell'operatore per una determinata attività.

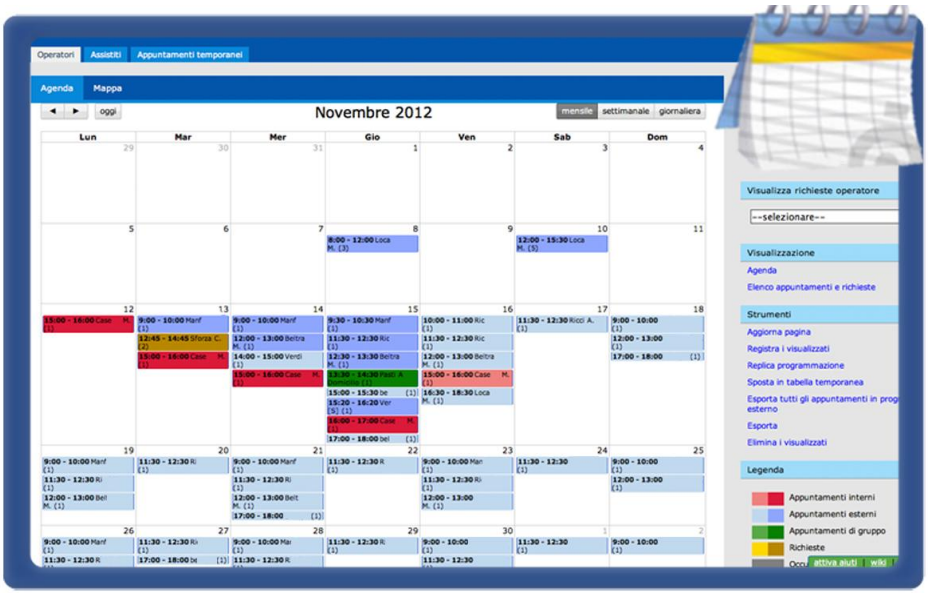

Figura 19: la pianificazione delle attività in Vitaever

Gestione dei dati clinici e diari

Vitaever consente anche la gestione di diversi dati clinici degli assistiti: dalla compilazione di diverse tipologie di cartelle cliniche (anamnesi, socio-assistenziali, multidimensionali, funzionali, ecc.), alla registrazione dei sintomi e delle problematiche di rilevanza medica (dolori, sonno, alimentazione, terapia).

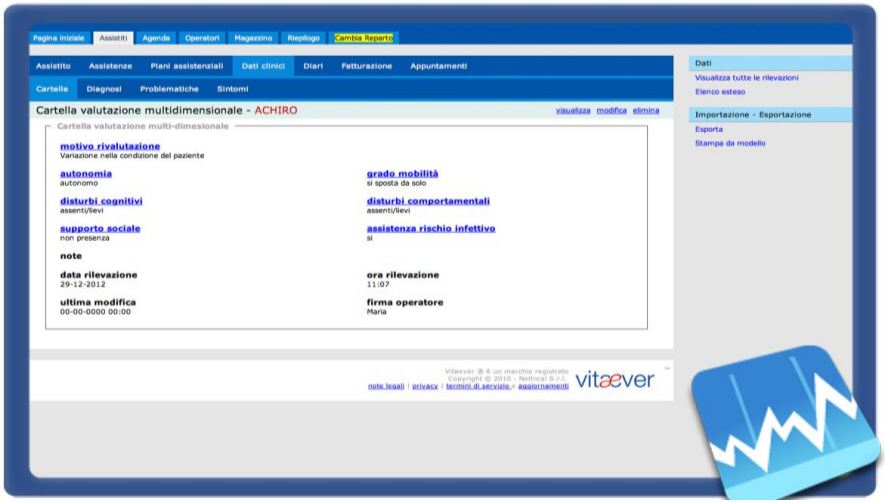

Figura 20: la gestione di una cartella clinica multidimensionale

Il sistema è in grado, altresì, di tenere traccia di tutte le informazioni passate e dell'utente che ha inserito o modificato l'informazione presente in banca dati.

Ad ogni assistito è associabile un diario, ovvero una sezione dove indicare le informazioni o commenti relativi agli interventi effettuati, alle problematiche riscontrate e all'assistenza prestata. La sezione del diario è consultabile e modificabile anche da altri operatori, dall'assistito e dai suoi familiari, in modo da consentire la condivisione rapida e agevole delle informazioni tra tutti i soggetti coinvolti nel processo di assistenza e cura.

Rilevazione presenze e geolocalizzazione

Grazie alla tecnologia QR-Code (*Quick Response Code*) implementata nella piattaforma, Vitaever è in grado di gestire e verificare le presenze presso il domicilio dell'assistito. Il sistema associa a ciascun assistito un QR-Code univoco e ciascun operatore potrà verificare la sua presenza, l'inizio o la fine dell'attività attraverso la semplice scansione del codice.

Un'altra funzionalità di Vitaever è la geolocalizzazione basata su tecnologia Google che consente agli operatori di calcolare e indicare il percorso migliore e più veloce per raggiungere il domicilio dell'assistito.

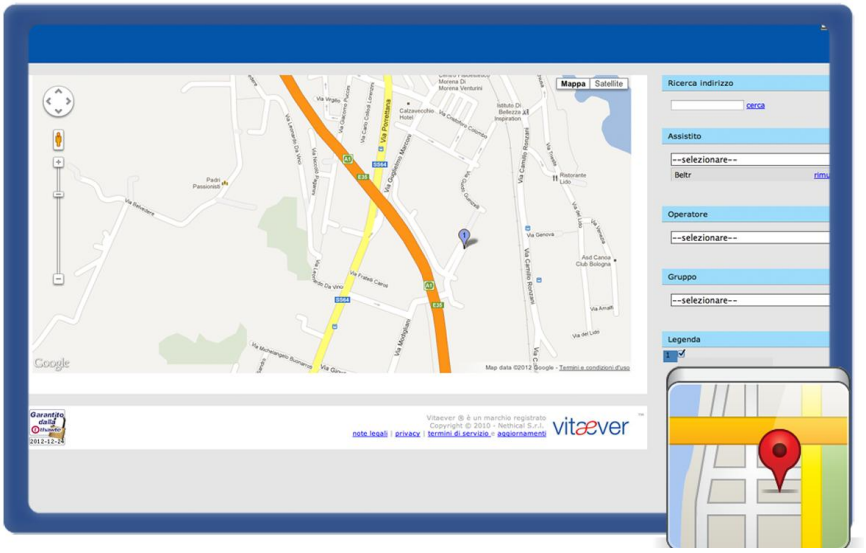

Figura 21: la geolocalizzazione con i servizi di Google

Gestione magazzini, fatturazione, rendicontazione e report.

Di particolare utilità è la possibilità di gestire i processi di ritiro e consegna dei farmaci, dei presidi e di altri beni consegnati agli assistiti, tenendo traccia di tutti gli spostamenti del materiale distribuito.

La piattaforma consente di gestire facilmente e in modo completo tutto il processo di rendicontazione e fatturazione delle attività svolte grazie alla possibilità di associare a ciascun assistito e operatore un profilo di fatturazione personalizzato e di generare il riepilogo dettagliato di tutti i costi relativi ai servizi prestati e ricevuti.

È, altresì, prevista la possibilità di gestire tutte le attività svolte dagli operatori, le risorse impiegate, le prestazioni erogate agli assistiti e i relativi costi. Tutte le informazioni sono esportabili in vari formati (excel, csv, xml, ics), garantendo l'interoperabilità e l'elaborazione delle informazioni anche attraverso *software* gestionali di terze parti.

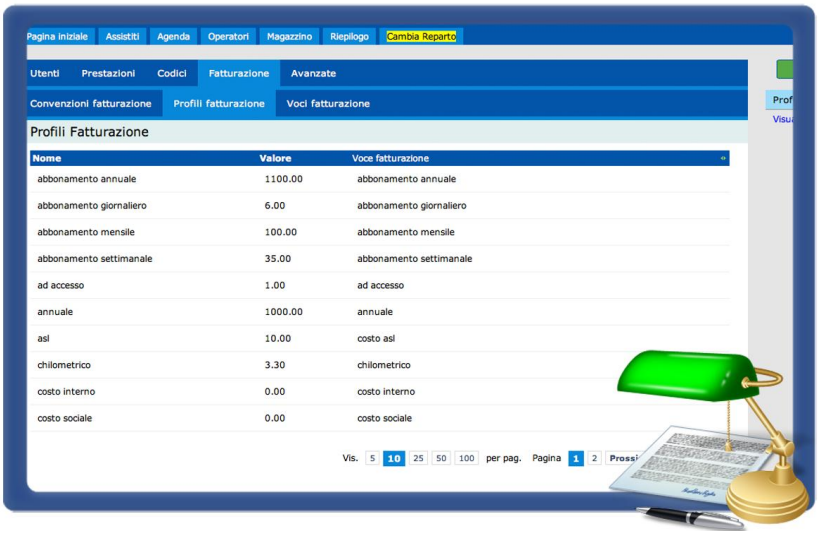

Figura 22: la gestione del profilo di fatturazione

Messaggistica, gestione allegati e stampe

Tutti gli utenti che popolano la piattaforma possono comunicare internamente attraverso un sistema di messaggistica che consente lo scambio sicuro di informazioni e allegati. L'accesso e la condivisione di documenti e allegati è consentita ai soli utenti in possesso di un profilo di accesso a ciò abilitato.

L'Amministratore del sistema può personalizzare i *layout* di stampa attraverso il caricamento di modelli in formato ".odt" (OpenOffice), definiti in base alle singole esigenze degli operatori.

L'accesso con dispositivi mobili

Vitaever è studiato ed organizzato in modo tale da consentire l'accesso al sistema sia mediante *personal computer*, sia attraverso dispositivi *mobile*,

(cellulari, *smartphone* o *tablet*), secondo il paradigma BYOD (*Bring Your Own Device*). Questa funzionalità consente, quindi, a ciascun operatore di avere costantemente accesso alle informazioni aggiornate degli assistiti e di gestire la propria attività da qualunque parte e in ogni momento.

2.2 Vitaever e *cloud computing*

Tutte le funzionalità sin qui descritte sono fornite mediante la tecnologia *Cloud* di tipo SaaS (*Software as a Service*), la quale consente di non dover necessariamente scaricare e installare il *software*. Grazie al paradigma BYOD, è utilizzabile da qualunque dispositivo fisso o mobile.

Inoltre, il modello SaaS non richiede l'implementazione di un'infrastruttura dedicata e, di conseguenza, non è necessario avere competenza tecniche particolari per garantirne il mantenimento nel tempo; in tal modo, grazie all'aumento della produttività ottenuto, si ottiene un rapido ritorno dell'investimento iniziale, già notevolmente contenuto.

La soluzione offerta da Vitaever consente di usufruire immediatamente dei servizi, senza dover sopportare i costi tradizionali del *software* quali l'acquisto e la manutenzione del *server*, la sicurezza delle informazioni e l'installazione di applicativi. Tale facilità di organizzazione e di utilizzo dei servizi consente all'organizzazione utente di focalizzarsi maggiormente sugli aspetti prettamente lavorativi di assistenza e cura degli assistiti.

Con Vitaever, come per tutte le applicazioni SaaS, si realizzano economie di scala. Le organizzazioni, pubbliche e private, che adottano questo sistema ottengono un rapido ritorno degli investimenti, aumentano la produttività e, grazie al sistema *Pay-as-you-go*, spendono in proporzione alla dimensione, al numero degli assistiti oppure degli appuntamenti svolti o del numero degli operatori coinvolti.

2.3 *Privacy*, sicurezza e vantaggi del *cloud* Vitaever

La sicurezza e gli aspetti legati alla *privacy* sono gestiti direttamente dal fornitore del servizio di *Cloud*, così da liberare i titolari del trattamento dai relativi oneri e costi legati all'implementazione di soluzioni in grado di ga-

rantire l'alto livello di affidabilità e sicurezza richiesta dalla piattaforma. Allo stesso modo, anche tutti gli oneri derivanti dall'aggiornamento, dalla gestione delle applicazioni e dall'implementazione di nuove funzionalità, non ricadono sul singolo utilizzatore.

La sicurezza e la protezione dei dati personali sono garantite attraverso l'uso di protocolli sicuri, *password* individuali e cifrate. In linea con le disposizioni in materia di trattamento di dati personali, il *cloud* Vitaever consente la visualizzazione e la modifica dei dati personali solamente agli utenti autorizzati. Il sistema di personalizzazione dei permessi, inoltre, consente di personalizzare i livelli di accesso garantendo ampia flessibilità nella gestione delle risorse, senza compromettere la sicurezza e la riservatezza delle informazioni[12].

Gli effetti positivi dell'adozione della soluzione *Cloud* Vitaever possono essere suddivisi in tre differenti aree: benefici diretti per le organizzazioni, benefici per i malati e gli anziani non autosufficienti e, infine, vantaggi indiretti legati al modello funzionale.

Per quanto concerne i primi è sufficiente analizzare quanto accaduto, nell'arco temporale di 12 mesi, alla Fondazione ANT Italia Onlus. Essa che conta circa 4000 assistiti e 300 operatori, grazie al contenimento dei costi di gestione dovuti alla riduzione dell'attività di *back office*, a fronte di un investimento di 42.000 € ha stimato un risparmio di 64.000 € (con un ritorno sugli investimenti del 150%). L'esperienza della Cooperativa Sociale La Spiga (300 assistiti e 80 operatori), dopo un anno di attività con Vitaever, ha evidenziato una riduzione del tempo speso dagli operatori in attività non a valore aggiunto; in termini di pianificazione, coordinamento e rendicontazione, è stato stimato un risparmio di 7/9 giorni lavorativi al mese.

I vantaggi per i malati e gli anziani non autosufficienti si concretizzano nel cosiddetto "*Empowerment* dell'assistito" ovvero nella sua maggiore inclusione nel processo di assistenza, grazie alla condivisione delle informazioni e dei dati clinici con medici di base e familiari. Inoltre, non è da sottovalutare la possibilità per gli operatori di essere sempre costantemente ag-

[12] Su tale versante, in virtù di una partnership con l'Università di Bologna sono state sviluppate ed implementate tecnologie in grado di eseguire la cifratura dei dati sensibili mediante chiavi private a livello di singola licenza, garantendo così la sicurezza e la riservatezza dei dati anche nei confronti di terzi.

giornati sulle condizioni di salute, sulla storia clinica e assistenziale dell'assistito.

Infine, i vantaggi indiretti dovuti alle caratteristiche funzionali del sistema *Cloud* Vitaever sono rappresentanti da una serie di aspetti eterogenei che di seguito si elencano:

- il passaggio dalla logica di rendicontazione a quella di gestione e monitoraggio del processo di assistenza;
- la diminuzione dei costi di gestione della cura a domicilio;
- l'abbassamento dei costi legati alla rendicontazione verso Enti territoriali e ASL, grazie all'automazione della stessa;
- il miglioramento della capacità di pianificare, anche a fronte di eventi improvvisi ed imprevedibili;
- la standardizzazione delle procedure che consente il rapido inserimento di nuovi operatori;
- l'informazione rapida e completa del personale dislocato nel territorio;
- la riduzione dei rischi legati alle attività critiche (passaggi di consegne, terapie, pianificazione della cura);
- la tracciabilità delle prestazioni;
- il miglioramento del controllo nella distribuzione dei presidi e dei farmaci;
- la disponibilità di dati e informazioni aggregati e strutturati per la ricerca in campo medico-scientifico;
- la *business intelligence*, o controllo di gestione attraverso i dati e i *report*;
- la possibilità di adottare delle *best practices*.

Appare doveroso concludere evidenziando che le soluzioni adottate sono state ritenute tra le tecnologie più sicure per le applicazioni in campo sanitario e hanno consentito il riconoscimento del Primo premio "*The Best Privacy Guardian*", ricevuto in occasione di Tecnosan 2013[13].

[13] Si è svolta nei giorni 15 e 16 marzo e si tratta della prima manifestazione "aperta" nella quale istituzioni, esperti del settore ed industrie telemedicali italiane si sono incontrati per discutere di numerose tematiche legate alla Sanità, in generale, ed alla Sanità elettronica in particolare.

3. Il progetto "eTriage"

Il progetto "Triage"[14] nasce da uno studio in cui hanno collaborato insieme l'Istituto Italiano per la *Privacy*, il CATTID de La Sapienza, la società Microsoft e il Centro Italiano per la Sanità Digitale ed è stato presentato per la prima volta il 5 dicembre 2012 a Bruxelles, in occasione del convegno "*Innovating for better health: doing New with Less*"[15].

Il progetto nasce dall'idea di realizzare il "triage" di pronto soccorso dei pazienti attraverso un sistema esperto collocato in una piattaforma *cloud*, mediante la rielaborazione di tutti i dati sanitari presenti nei sistemi del Servizio Sanitario Nazionale e relativi alla storia clinica di ciascun paziente.

Com'è noto il "triage" è un sistema utilizzato per la selezione dei soggetti coinvolti in infortuni secondo varie classi di emergenza che tengono conto sia delle lesioni riportate che del quadro clinico complessivo. É utilizzato innanzitutto presso i presidi di pronto soccorso per garantire un accesso alle cure non secondo l'ordine di arrivo ma in base alla gravità delle condizioni dei pazienti, a cui viene assegnato un codice colore (bianco, verde, giallo, rosso).

Con il progetto "Triage" questa procedura di valutazione ed assegnazione della priorità avviene con modalità automatizzate, grazie al lavoro di rielaborazione eseguito da un sistema informatico sui dati sanitari relativi ai casi pregressi di ciascun paziente e alle informazioni raccolte nell'immediato.

L'obiettivo del progetto non è quello di realizzare un sistema in grado di sostituirsi al lavoro del medico, bensì di creare un'infrastruttura in grado di coadiuvarlo, nell'attività di pronto soccorso, nella valutazione del paziente, soprattutto nelle situazioni in cui, per varie ragioni, il presidio sanitario non abbia le capacità organizzative o professionali per fornire un servizio

[14] Cfr. L. BOLOGNINI, D. FULCO, E. PELINO, *Dati sanitari e* Cloud Computing *per finalità di triage di pronto soccorso: profili e criticità in materia di protezione dei dati personali*, Istituto Italiano per la Privacy e F. BARTOLI, C. M. MEDAGLIA, *Il riutilizzo dei dati nel settore della sanità pubblica: il progetto e-triage* "triage on the cloud", CATTID, Università Sapienza di Roma, 2012. Consultabile all'indirizzo web: http://www.vecchioistitutoprivacy.dwb.it/it/Cloud_sanitario_Triage_ITA_CATTID_IIP_MS_2012.pdf.

[15] In Italia è stato presentato per la prima volta nel 2013 a Roma presso la sede del Parlamento Italiano.

adeguato. Il *cloud computing*, in tale contesto, è stato considerato, dagli sviluppatori del progetto, l'unica soluzione tecnologica adottabile per consentire allo stesso tempo il riuso e l'elaborazione di una mole così complessa di dati sanitari.

L'infrastruttura, essendo progettata per operare sui dati sanitari[16] di numerosi soggetti, per essere spendibile su mercato deve necessariamente essere analizzata ed implementata in conformità alla disciplina giuridica in materia di protezione dei dati personali.

Così, in armonia con lo spirito "*data protection by design and by default*"[17], nello sviluppo del progetto "Triage" sono stati affrontati tutti gli aspetti critici delle infrastrutture *cloud* in applicazione al settore sanitario, dalle questioni tecnologiche a quelle giuridiche legate alla *privacy*. Lo studio elaborato intorno al suddetto progetto, oltre a rappresentare un importante passo in avanti per la ricerca giuridica e informatica sul tema, costituisce un valido punto di riferimento per gli operatori del settore intenzionati ad attivare altre iniziative analoghe in Italia e in Europa.

È proprio in applicazione del "*data protection by design and by default*", che l'achitettura dell'intero sistema "Triage" è stata ispirata alla minimizzazione dei dati ("*data minimisation*") da intenedere come limitazione del trattamento a quanto necessario rispetto alle finalità per perseguite. Detto principio, oltre ad avere un impatto positivo nell'economia e nella gestione del progetto, costituisce un vero e proprio obbligo di legge, sancito all'art. 3 del D. Lgs. 30 giugno 2003, n. 196 e all'art. 5, lett. c) e 25 del nuovo Regolamento UE 679/2016.

Come meglio si approfondirà nel prosieguo, la soluzione adottata nel sistema "Triage" consiste nell'anonimizzazione dei dati sin dalla fase iniziale del flusso informativo che alimenta il *database* primario, così da consentire la circolazione all'interno dell'infrastruttura *cloud* delle sole informazioni dissociate dalla componente identificativa.

[16] Con il termine "dati sanitari" si indicano tutti i dati idonei a rivelare lo stato di salute del soggetto interessato.

[17] Sul concetto di "*data protection by design and by default*" si rimanda a quando illustrato nella parte terza e quarta del presente lavoro.

3.1 Struttura e obiettivi principali del Progetto

Il progetto "Triage" intende realizzare un'infrastruttura in grado di fornire le informazioni sanitarie ai presidi di pronto soccorso durante la fase di assegnazione dei codici di *triage*[18]. Sostanzialmente il sistema opera il "*matching*" tra i dati sanitari storici del paziente e i dati relativi ai sintomi e all'anamnesi immessi dall'operatore sanitario del pronto soccorso. I dati storici del paziente, unitamente alle diagnosi a loro associate, sono elaborati in chiave statistica dal sistema e resi fruibili al personale curante che potrà utilizzarli per assegnare un codice di *triage* che tenga conto anche delle pregresse situazioni cliniche del paziente, così da assicurargli in breve tempo un processo di cura ed assistenza più adeguato. Le informazioni di *output* fornite con questo sistema, quindi, consentono di migliorare l'efficienza e la tempistica delle operazioni di *triage* e rappresentano, da un lato, uno strumento di integrazione delle diagnosi del personale sanitario e, dall'altro, un valido strumento per consentire alle amministrazioni sanitarie un miglioramento dell'organizzazione dei reparti di pronto soccorso.

Tenuto conto degli obiettivi e delle caratteristiche del progetto, le parti coinvolte nello studio hanno individuato il *cloud computing* quale soluzione più adatta per l'immagazzinamento dei dati nel *database* e per la gestione dei flussi informativi, anche in virtù dei vantaggi economici e dell'efficienza in generale.

L'architettura, nel suo complesso, prevede un *database* centrale e condiviso in cui sono immessi i dati e le informazioni sanitarie relativi ai processi di cura già realizzati da ciascun presidio di pronto soccorso e in possesso dei vari organismi sanitari che partecipano alla realizzazione del progetto, definiti "*provider*". Per ciascun *provider* si realizzano, così, due flussi di dati: uno in entrata, dal paziente in ingresso nel pronto soccorso al *provider*, e uno in uscita, dal provider al *database* centrale del sistema "Triage". Non dovrebbero, invece, realizzarsi flussi di dati "orizzontali"[19], così semplificando notevolmente il trattamento dei dati e la definizione dei

[18] Nell'ambito dell'architettura del sistema, le informazioni fornite agli operatori sanitari vengono definite semplicemente "*output*".

[19] I flussi cosiddetti orizzontali sono quelli determinati dalla comunicazione di dati da *provider* a *provider*.

ruoli in ambito *privacy*. Un terzo ed ultimo flusso informativo si realizza quando il dato del paziente viene restituito alla struttura sanitaria e all'operatore di pronto soccorso impegnato nell'assegnazione del codice di *triage*.

Alla luce dell'architettura e dei flussi informativi descritti, le parti coinvolte nel progetto hanno convenuto di realizzare l'anonimizzazione del dato sin dalla fase di gestione dello stesso da parte del *provider*, prima che sia immesso all'interno del *database* condiviso. La trasformazione in forma anonima è eseguita direttamente dal *provider*, seguendo un protocollo comune a tutte le strutture aderenti al progetto. La scelta del momento in cui realizzare l'anonimizzazione dei dati è fondamentale, in quanto comporta rilevanti conseguenze sia sull'intera architettura del progetto, sia sulle risultanze statistiche dello stesso[20].

3.1.1 Architettura

Per consentire alle strutture ospedaliere di utilizare i dati da loro raccolti e fornirli in modo anonimo per l'erogazione di servizi di teleassistenza, di primo intervento ed emergenza nell'ambito di piccoli ospedali e nelle autoambulanze deputate alle prime cure del paziente, spesso decisive e determinanti nell'efficacia dei successivi processi di cura, i dati del sistema sono memorizzati in una grande banca dati *cloud* senza essere associati all'identità personale dei pazienti a cui si riferiscono, tutelando così la loro riservatezza e, allo stesso tempo, permettendo il trattamento delle informazioni senza le limitazioni previste per i dati di natura sanitaria.

Le informazioni personali degli utenti/pazienti sono conservate localmente all'interno della singola struttura ospedaliera che assume il ruolo di *data provider* e presso la quale il paziente si è rivolto per ottenere le cure necessarie. In tal modo, l'identità anagrafica del paziente è sganciata dalle informazioni sensibili per consentirne il riuso da parte di altre strutture sanitarie senza i vincoli previsti dal nostro ordinamento per il trattamento dei dati di tale natura.

[20] L'anonimizzazione dei dati in un momento antecedente la loro immissione nel *database*, infatti, non consentirebbe una loro eventuale correzione necessaria per meglio definire il quadro sanitario del paziente.

3.2 Classificazioni e *standard* utilizzati

Per la definizione delle specifiche tecniche del progetto si è proceduto alla definizione dei requisiti del sistema, attraverso tre principali *step*: il primo è consistito nell'identificazione dei potenziali attori e fruitori della piattaforma; il secondo è stato quello della individuazione delle aspettative funzionali, di sicurezza e di usabilità; successivamente, sulla base delle valutazioni ricavate dai precedenti *step*; si è proceduto all'individuazione dei requisiti essenziali sottoelencati.

Requisiti Funzionali: l'insieme delle azioni e funzioni che necessariamente devono essere implementate nel sistema affinchè siano generati *output* appropriati.

Requisiti dei Dati: l'insieme delle condizioni previste per il contenuto e la semantica dei dati, indipendentemente dal formato utilizzato. Tali requisiti devono sussistere al di là della tipologia di *database* utilizzato.

Requisiti di Interoperabilità: individuano la capacità del sistema di condividere le informazioni e i servizi attraverso l'impiego di interfacce in grado di garantire l'interoperabilità con altri sistemi esterni. Inoltre, essi riguardano anche le caratteristiche degli *standard* necessari per consentire l'interoperabilità.

Requisiti di Usabilità: rappresentano la capacità del sistema di essere facilmente utilizzato grazie all'uso di interfacce intuitive e facili all'apprendimento.

Requisiti di Operatività: individuano le condizioni e i livelli di prestazione e funzionamento della piattaforma.

Requisiti di Sicurezza: tutti gli elementi essenziali atti a proteggere la piattaforma da modifiche non autorizzate, usi non consentiti, accessi abusivi o accidentali. Ne sono un esempio l'uso di sistemi di cifratura, restrizioni delle comunicazioni e così via.

Requisiti Legali: specificano le condizioni previste in ragione di una normativa specifica ed applicabile al settore interessato.

Sussistono tre differenti livelli: il primo livello è "essenziale" e indica che il sistema deve essere obbligatoriamente implementato secondo quel requisito; il secondo livello è "condizionale" ed è attribuito al requisito che, pur non essendo necessario, comunque aumenterebbe la capacità e il valore

del sistema. Infine, il requisito o la funzione è definita di livello "opzionale" quando la sua implementazione consente di fornire qualcosa in più rispetto ai requisiti richiesti.

Per quanto attiene, infine, agli *standard* di codifica, il progetto eTriage utilizza il sistema ICD-9-CM (*International Classification of Diseases - 9th revision - Clinical Modification*)[21], riconosciuto e adottato, a partire dal 2009, dal Ministero della Salute per l'inserimento delle informazioni cliniche nella SDO (Scheda di Dimissione Ospedaliera) e nelle altre diagnosi effettuate dagli operatori sanitari.

3.2.1 Protocolli di comunicazione e implementazione del *database* eTriage

Lo scambio di dati nell'ambito del sistema eTriage avviene sulla base del protocollo HL7 che costituisce lo *standard* internazionale più diffuso nel settore dell'*e-Health*.

Il protocollo suddetto è in grado di descrivere le interfacce tra applicazioni diverse, di contenere le definizioni dei dati da condividere e altre informazioni sullo stato della comunicazione. L'uso di HL7 consente, altresì, la comunicazione di dati sanitari relativi ad un singolo paziente tra applicazioni e interfacce diverse, permettendo quindi l'interoperabilità tra i vari sistemi sanitari.

In questo modo il sistema eTriage acquisisce maggiore flessibilità, potendo ospitare un numero illimitato di interfacce e, di conseguenza, di *data provider*.

Nella figura 23 è illustrato il modello logico del *database* eTriage secondo i requisiti e gli *standard* fin qui descritti.

[21] La Classificazione internazionale delle malattie (ICD) è un sistema di classificazione delle malattie e dei traumatismi in gruppi tra loro correlati ed è finalizzata a tradurre in codici alfa-numerici i termini medici relativi alle diagnosi. Con tale sistema sono catalogate e classificate anche le procedure diagnostiche e terapeutiche e gli interventi. Attualmente, in Italia è in uso la versione ICD-9-CM 2007.

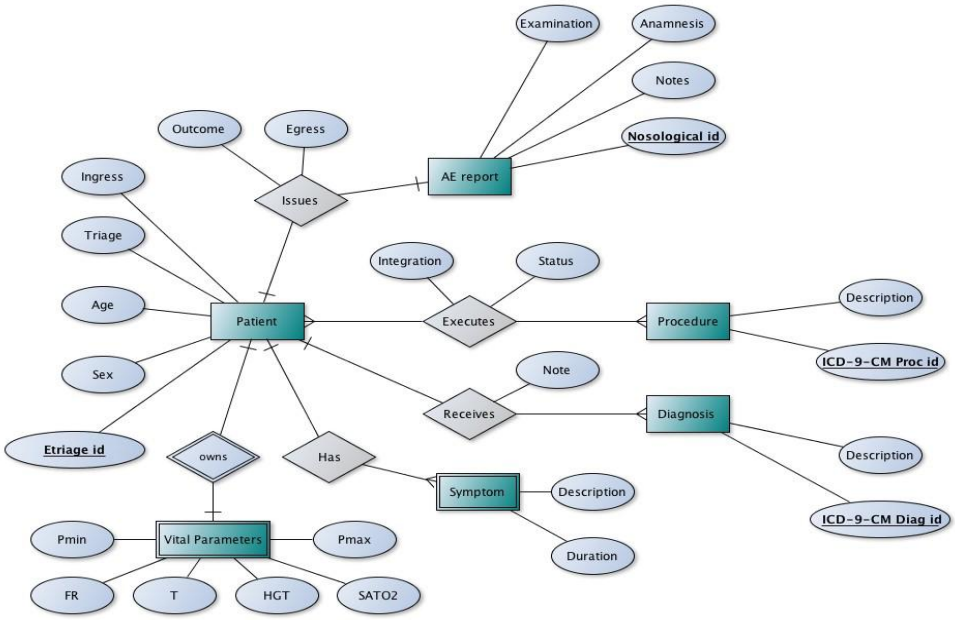

Figura 23: Modello logico del *database* eTriage[22]

Si può notare come il paziente costituisca il punto cardine dell'intera struttura e come lo stesso venga descritto attraverso informazioni, rilevanti ai fini della compilazione della cartella di Pronto soccorso, senza far riferimento a dati personali identificativi. Come già detto al paragrafo precedente, si segue lo standard di codifica ICD-9-CM.

La figura 24 mostra come è stata riprodotta la complessa struttura del sistema di codifica ICD-9-CM sul database di SQL Azure:

[22] Fonte: F. BARTOLI, C. M. MEDAGLIA, *Il riutilizzo dei dati nel settore della sanità pubblica: il progetto e-triage "*triage on the cloud*"*, CATTID, Università Sapienza di Roma, p. 37

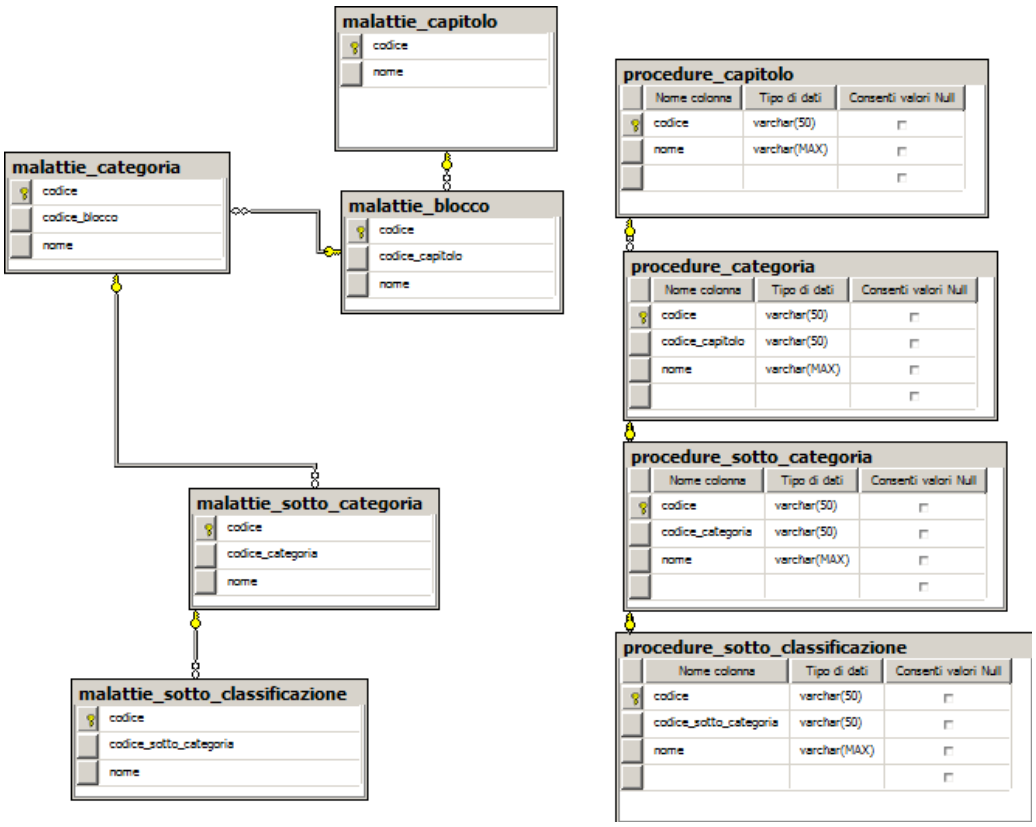

Figura 24: Codifiche delle malattie e procedure ICD-9-CM[23]

3.2.2 Implementazione Servizi eTriage: il cloud di Windows Azure

Il progetto eTriage è stato realizzato attraverso i servizi *cloud computing* di Windows Azure. Questa piattaforma *cloud* consente di compilare, gestire e distribuire applicazioni in modo facile e veloce, grazie alle sue caratteristiche di apertura e flessibilità.

Inoltre, Windows Azure consente di compilare applicazioni con tutti i linguaggi di programmazione, con qualsiasi strumento o *framework* e permette di integrare le applicazioni del *cloud* pubblico con l'ambiente IT già esistente. L'aggiornamento dell'applicazione *cloud* avviene senza tempi di inattività.

I servizi forniti dalla piattaforma prevedono il rilascio di una applicazione di *patch* automatica al sistema operativo e ai servizi, il

[23] Fonte: F. BARTOLI, C. M. MEDAGLIA, *Il riutilizzo dei dati nel settore della sanità pubblica: il progetto e-triage* "triage on the cloud", CATTID, Università Sapienza di Roma, p. 39

bilanciamento del carico di rete predefinito e la resilienza agli errori *hardware*.

L'intera architettura di Windows Azure è progettata per offrire servizi *on-demand* in modalità *cloud* attraverso l'impiego di diversi *data center* dislocati in varie parti del globo, dagli Stati Uniti, all'Europa e all'Asia, ed è basata sulla virtualizzazione delle risorse fisiche. Ciò consente la scalabilità sia verticale che orizzontale dei servizi offerti.

Con Windows Azure è possibile attivare differenti servizi di *cloud* che vanno dal semplice *storage* al servizio di *hosting* fino ad arrivare ai servizi di piattaforma per lo sviluppo delle applicazioni[24]; infine, è anche offerto il servizio di SQL Azure, una versione di SQL Server in ambiente *cloud*.

Il servizio di *storage* è denominato *Windows Azure Storage Service* e consente di archiviare i dati in modo persistente e durevole in una piattaforma accessibile da qualsiasi applicazione. Tra le funzionalità più rilevanti vi è la possibilità di memorizzazione dei dati in forma tabellare[25] e di *file* binari (come documenti e immagini)[26], di creare code di messaggi tra componenti di una soluzione[27] e, infine, di sfruttare le funzionalità di un *file system* remoto grazie al *Drive Storage Services*.

Il servizio di *hosting*, denominato *Windows Azure Hosted Services* consente di sviluppare qualsiasi applicazione *web-based* o di *back-end* con l'uso delle principali tecnologie .NET, JAVA e PHP.

3.3 I soggetti e le finalità del progetto eTriage

Alla base del progetto eTriage vi sono i cd. P*rovider*, organismi sanitari sia pubblici sia privati[28], che rappresentano i soggetti "attivi" del trattamento in riferimento ai dati dei pazienti.

In applicazione dell'art. 28 del Codice *Privacy*, il titolare del trattamento va individuato nella struttura sanitaria e non nel singolo reparto di pronto

[24] *Windows Azure platform AppFabric*

[25] *Table Storage Services*

[26] *Blob Storage Services*

[27] *Queue Storage Services*

[28] Anche i privati possono fornire servizi di assistenza e cura di pronto soccorso. Tuttavia, la loro attività, essendo regolata su base regionale, potrebbe differire di regione in regione.

soccorso, salvo che quest'ultimo non eserciti un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, compreso il profilo della sicurezza. In tal caso, il reparto di pronto soccorso sarà inquadrato quale titolare.

Qualora vi sia un ente centrale deputato alla gestione del *database* condiviso, avente poteri di decisione in merito alle finalità e alle modalità di aggregazione e di elaborazione dei dati, anche questo potrebbe essere inquadrato quale soggetto "attivo" del trattamento.

Tuttavia, la scelta di progettare un sistema in cui tutti i dati immessi nel database centrale sono già resi anonimi consente di escludere la presenza di attività di trattamento e, quindi, di non considerare "attiva" la posizione di un eventuale ente gestore della base di dati condivisa[29].

I soggetti "passivi" sono tutti i soggetti che subiscono il trattamento dei propri dati da parte delle strutture sanitarie, inquadrati come "interessati" dal Codice *Privacy*[30], e possono essere suddivisi in due differenti tipologie. Da una parte, vi sono tutti i pazienti di pronto soccorso che in passato si sono rivolti alla struttura sanitaria[31], in riferimento ai quali esiste una documentazione medica in possesso della stessa struttura; le informazioni ivi contenute costituiscono il primo flusso di dati dell'architettura di eTriage, dal paziente al *provider*. Dall'altra, vi sono i pazienti, cosiddetti "attuali", ai quali il pronto soccorso fornisce l'assistenza necessaria sfruttando l'*output* dell'infrastruttura eTriage. I pazienti "attuali" possono anche essere pazienti "storici" già curati nella stessa struttura sanitaria oppure possono divenire "storici" nel momento in cui le informazioni a loro riferite sono immesse all'interno dei flussi di dati previsti da eTriage.

L'analisi delle finalità del progetto eTriage rappresenta un passaggio rilevante soprattutto per le implicazioni di natura giuridica connesse al trattamento dei dati.

---

[29] Il dato anonimo, infatti, non rientra nella definizione di dato personale ai sensi dell'art. 4, lett. b) del D. Lgs. 196/2003. Il trattamento, quale attività effettuata sui dati e rientrante nelle operazioni elencate nell'art. 4, lett. a), non può sussistere nel caso dei dati anonimi, essendo venuta meno proprio la qualità di dato personale.

[30] In base alla definizione dell'art. 4, comma 1, lett. i) l'interessato è "la persona fisica cui si riferiscono i dati personali"

[31] Per queste ragioni si definiscono pazienti "storici".

Ogni progetto in materia di sanità elettronica, a seconda dell'impostazione data e degli obiettivi che si intendono raggiungere, può rispondere a finalità differenti: dalla semplice cura dei pazienti, alla gestione amministrativa, fino ad arrivare a finalità di ricerca medica e statistica. In particolare, come è già stato illustrato, il progetto eTriage risponde contemporaneamente a due specifiche esigenze: l'integrazione delle diagnosi di pronto soccorso e la programmazione della gestione amministrativa delle attività dei reparti di pronto soccorso. Entrambe rientrano pacificamente tra le finalità di rilevante interesse pubblico previste dall'art. 85, comma 1 e 2, del Codice *Privacy*.

Nel progetto, quindi, restano escluse le finalità di ricerca e statistica. Infatti, l'obiettivo principale che si intende perseguire è quello di fornire agli operatori sanitari uno strumento di ausilio per ridurre i tempi di elaborazione delle diagnosi di pronto soccorso, ottenendo così numerosi benefici in termini di efficienza e gestione dell'utente. In questo contesto, eventuali nuove conoscenze acquisite con le risultanze di *output* del progetto costituirebbero, infatti, mere scoperte occasionali atipiche. Anche le elaborazioni statistiche presenti nel sistema eTriage rappresentano solamente uno strumento finalizzato al raggiungimento degli obiettivi sopra descritti, e non una finalità vera e propria del progetto.

3.4 Le principali questioni giuridiche

Le principali questioni giuridiche legate al progetto eTriage ruotano attorno ai profili di liceità del trattamento dei dati e delle informazioni, alle condizioni e agli adempimenti richiesti dalla normativa a tutela dei dati personali.

Gli aspetti di maggior rilievo che sono stati analizzati riguardano la finalità del trattamento, l'informativa, il consenso dell'interessato e l'autorizzazione del Garante *Privacy*. In particolare, se da una parte l'informativa è sempre prevista, dall'altra il consenso e la richiesta di autorizzazione sono adempimenti richiesti solo in specifici casi, tenuto conto della finalità perseguita e la natura pubblica o privata della struttura sanitaria, titolare del trattamento.

Prima di affrontare nello specifico ogni aspetto giuridico, è bene mettere in evidenza una peculiarità del progetto in relazione ai ruoli dei soggetti e al loro inquadramento nel Codice *Privacy* e nel neonato Regolamento Generale sulla Protezione dei Dati. Infatti, nell'ambito del sistema eTriage si può realizzare una dissociazione tra soggetto interessato e soggetto destinatario del trattamento, che determina qualche differenza a livello di disciplina legale.

La dissociazione opera in questo senso: nel primo caso, cosiddetto modello "normale" (o "associato") il soggetto interessato è anche destinatario della prestazione erogata dal pronto soccorso e, quindi, dal sistema eTriage; nel secondo caso, o "modello dissociato", l'interessato non è destinatario della prestazione del pronto soccorso. In altre parole, la dissociazione si realizza ogni qual volta un paziente del pronto soccorso è terzo rispetto ai soggetti storici, ovvero quelli che hanno già ricevuto in passato una prestazione medica in pronto soccorso.

3.4.1 L'informativa e il consenso nel trattamento dei dati sanitari

Nell'approccio alla disciplina in materia di protezione di dati personali, il D.lgs. distingue gli organismi sanitari pubblici da quelli privati. Sul piano della liceità del trattamento, mentre i primi sono vincolati al principio di legalità, i secondi necessitano della manifestazione del consenso da parte dell'interessato.

Nel Codice *privacy* si individuano, per i soggetti pubblici, tre differenti ipotesi di trattamento dei dati sensibili (e quindi sanitari)[32]:

a) I soggetti pubblici possono trattare dati sensibili solo se autorizzati da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, i tipi di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
b) Se la disposizione di legge specifica solamente la finalità di rilevante interesse pubblico ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo se i soggetti pubblici hanno provveduto ad individuare e rendere pubblici i tipi di dati e di

[32] Cfr. art. 20, comma 1, D. Lgs. 196/2003

operazioni di trattamento, in relazione alle specifiche finalità perseguite nei singoli casi[33].

c) Se un particolare trattamento non è previsto da alcuna norma di legge, i soggetti pubblici possono richiedere al Garante di individuare tra le varie attività ad essi demandate dalla legge, quelle che perseguono una finalità di rilevante interesse pubblico e "*per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili*"[34]. Anche in questo caso, come nel precedente, il soggetto pubblico dovrà procedere ad individuare e rendere pubblici i dati e le operazioni di trattamento con atto di natura regolamentare e in conformità al parere del Garante.

Il trattamento dei dati sensibili (e quindi sanitari) da parte dei soggetti privati può essere effettuato solo con il consenso espresso del soggetto interessato e previa autorizzazione del Garante[35]. Il consenso non è richiesto quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato o di un terzo. Per i dati sanitari, ovvero quelli idonei a rivelare lo stato di salute, è previsto un divieto generale di diffusione.

Entrando più nello specifico, i trattamenti effettuati dagli organismi sanitari pubblici si distinguono in due tipologie: da una parte i trattamenti per finalità di tutela della salute e dell'incolumità dell'interessato, di un terzo o della collettività[36], dall'altra i trattamenti che perseguono finalità di rilevante interesse pubblico, individuate dagli artt. 85 e 86 del Codice *Privacy*. Quando il trattamento è effettuato per finalità diverse, ovvero hanno ad oggetto dati sensibili diversi da quelli sanitari, si applicano le disposizioni generali di cui all'art. 20 del Codice *privacy*.

I soggetti pubblici possono procedere al trattamento dei dati sanitari senza il consenso dell'interessato; questo può avvenire solo in presenza di

[33] L'individuazione va fatta nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare da adottarsi conformemente al previo parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g). Cfr. art. 20, comma 2, D. Lgs. 196/2003.

[34] Art. 20, comma 3, D. Lgs. 196/2003.

[35] Cfr. art. 26, D. Lgs. 196/2003.

[36] Cfr. art. 76, D. Lgs. 196/2003.

una specifica disposizione di legge che determini la finalità, i tipi di dati e le operazioni di trattamento consentite.

Per quanto concerne, invece, gli organismi sanitari privati il trattamento da loro effettuato deve sempre essere preceduto dal consenso espresso dell'interessato e dall'autorizzazione del Garante *privacy*.

Riportando l'analisi, sin qui svolta, al progetto eTriage, è necessario fare una distinzione a seconda che ricorra il modello normale, o "associato", ovvero quello cosiddetto "dissociato".

Nel primo caso, quando il soggetto interessato coincide anche con il soggetto destinatario della prestazione di pronto soccorso, qualora l'organismo sanitario sia un soggetto privato, il trattamento è consentito solo con il consenso dell'interessato e previa autorizzazione del Garante, mentre nel caso di soggetto pubblico è sufficiente il consenso dell'interessato[37]. Qualora l'interessato non sia nelle condizioni di poter prestare il proprio consenso, questo è prestato da altri soggetti individuati dal Codice *Privacy*.

Nel modello "dissociato", ossia quando l'interessato non coincide con il destinatario della prestazione, nella sostanza la disciplina applicabile è pressochè identica sia che si tratti di organismo pubblico che privato. Entrambe gli organismi, infatti, devono effettuare il trattamento previa autorizzazione del Garante e non sono tenuti a raccogliere il consenso dell'interessato[38].

L'autorizzazione a cui si fa riferimento è un atto amministrativo che l'Autorità Garante emana su richiesta del titolare del trattamento, ogni qual volta deve procedere ad un trattamento per il quale è previsto tale adempimento. Tuttavia, ai sensi dell'art. 40 del Codice *privacy*, la stessa Autorità ha previsto le autorizzazioni generali, che esonerano il titolare dall'obbligo di richiedere l'autorizzazione. Attualmente, il provvedimento in vigore e applicabile alle esigenze del progetto eTriage è l'autorizzazione generale n. 2/2014, valida fino al 31 dicembre 2016[39].

---

[37] La finalità perseguita è sempre quella di tutela della salute e dell'incolumità fisica.

[38] La normativa di riferimento è contenuta negli artt. 26, comma. 4, lett. b) e 76 del D. Lgs. 196/2003.

[39] Autorizzazione n. 2/2014 – "*Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*" - Registro dei provvedimenti n. 584 dell'11 dicembre 2014 (*Pubblicato sulla Gazzetta Ufficiale n. 301 del 30 dicembre 2014*) - doc. web n. 3619954

Il nuovo Regolamento UE 679/2016, ha parzialmente modificato la disciplina relativa al trattamento dei dati sensibili, prevedendo all'art. 9 un divieto generale di trattamento dei dati personali che rivelino, tra gli altri, dati relativi alla salute dell'interessato. Tale divieto non si applica quando ricorrono determinati casi, tra cui:

"[…] *h) il trattamento è necessario per finalità di prevenzione medica o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità;*

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale [...]".

Tale disposizione va integrata con quanto contenuto nell'art. 36 RGPD, che prevede il nuovo istituto della consultazione preventiva. Al comma 5 e riconosciuto il diritto degli Stati membri di prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Per quanto riguarda l'informativa nei confronti dell'interessato, nel Codice *privacy* sono previste delle modalità semplificate per gli organimi sanitari. Innanzitutto, occorre sottolienare come l'obbligo di fornire l'informativa grava su tutti i soggetti, sia pubblici che privati, e deve essere assolto prima della prestazione del consenso da parte dell'interessato. Quando la legge esclude l'obbligo di richiedere il consenso deve comunque essere fornita l'informativa al paziente.

In generale, il medico di medicina generale o il pediatra di libera scelta devono informare l'interessato in forma chiara e tale da rendere agevolmente comprensibili le finalità, le modalità del trattamento e i diritti che la legge riconosce all'interessato; inoltre, l'informativa deve specificare la natura

obbligatoria o facoltativa del conferimento dei dati in relazione alle finalità per le quali il paziente si rivolge alla struttura sanitaria, deve far riferimento alle conseguenze di un eventuale rifiuto e deve informare il paziente sui soggetti ai quali i suoi dati potranno essere comunicati o che possono venirne a conoscenza[40].

Le modalità semplificate, previste dall'art. 77 e ss. del Codice *Privacy*, consentono di fornire un'informativa che faccia riferimento a più trattamenti necessari, nella possibilità che la stessa sia fornita a vantaggio di più titolari del trattamento e nelle modalità con cui la stessa informativa può essere sottoposta all'interessato. L'intento del legislatore è quello di non caricare le strutture sanitarie e i medici con eccessivi adempimenti burocratici, pur garantendo allo stesso tempo la tutela dell'interessato.

In questa sede, assume un certo rilievo la disposizione di cui all'art. 78, comma 5, lett. c) che prevede l'obbligo di informare l'interessato circa i rischi specifici per i diritti, le libertà fondamentali e la dignità dello stesso, in relazione a trattamenti effettuati per fornire beni e servizi attraverso una rete di comunicazione elettronica.

In riferimento al progetto, l'informativa sul trattamento effettuato dai vari *provider*, organismi pubblici e privati, per le attività previste dal sistema eTriage deve essere necessariamente fornita in un momento successivo, ad integrazione dell'informativa fornita al paziente al momento della raccolta dei dati da parte della prima struttura sanitaria alla quale si è rivolto. È evidente che tale adempimento comporterebbe un notevole aumento dei costi e una difficoltà nell'organizzazione del progetto.

A tal proposito, si potrebbe ipotizzare l'applicazione dell'art. 13, comma 5, del Codice *Privacy* che consente di non fornire l'informativa "successiva" nel caso in cui comporti "*un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile*". La disposizione in commento, tuttavia, non si ritiene pienamente applicabile alle strutture sanitarie del progetto eTriage, poiché la

[40] Il contenuto dell'informativa è previsto e disciplinato dall'art. 13, D. Lgs. 196/2003.

stessa norma si riferisce al caso in cui l'informativa successiva è resa da un titolare diverso da quello che ha proceduto alla raccolta del dato[41].

Il Regolamento UE 679/2016, rispetto alla normativa suddetta assume sempre una rilevanza fondamentale ed anzi le informazioni da fornire sono anche maggiori e più dettagliate. Infatti, gli obblighi informativi sono distinti, negli articoli 13 e 14, tra i trattamenti di dati raccolti presso l'interessato e quelli che non siano stati ottenuti presso il medesimo.

Venendo ora al consenso, esso è previsto e disciplinato dall'art. 23 del Codice *Privacy*. Tuttavia, per i trattamenti effettuati in ambito sanitario sono previste delle modalità semplificate anche per il consenso.

In particolare, il consenso deve essere espresso[42], libero[43] e informato[44]. La semplificazione prevista dall'art. 81 del Codice *privacy* prevede che il consenso possa essere prestato anche oralmente, in deroga alla regola generale che richiede il consenso scritto, e deve essere annotato dall'organismo sanitario[45].

All'art. 7 del Regolamento privacy, in materia di consenso, si prevede che qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali.

Tale disposizione va coordinata con il divieto generale di trattamento di dati sensibili, quindi anche sanitari, contenuta nell'art. 9 del Regolamento, che è derogato, tra gli altri, nel caso in cui:

"*a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il*

---

[41] Per maggiori approfondimenti cfr. L. BOLOGNINI, D. FULCO, E. PELINO, *Dati sanitari e Cloud Computing per finalità di triage di pronto soccorso: profili e criticità in materia di protezione dei dati personali*, Istituto Italiano per la Privacy, 2012

[42] Non è ritenuto valido il consenso tacito o per comportamenti concludenti.

[43] Deve essere prestato senza condizionamenti o pressioni psicologiche

[44] Ovvero sempre preceduto dall'informativa.

[45] L'articolo 81, D. Lgs. 196/2003, prevede che "*Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, nei casi in cui è necessario ai sensi del presente codice o di altra disposizione di legge, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80*".

diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; […]
c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso".

3.4.2 Anonimizzazione dei dati

Alla luce delle considerazioni sin qui svolte, appare evidente come la disciplina applicabile agli organismi sanitari pubblici e privati, unitamente alla complessità generale del sistema, rappresentano un ostacolo allo sviluppo e alla diffusione del progetto eTriage nell'ambito dell'intero sistema sanitario nazionale Ciò vale anche in termini di costi e di difficoltà di gestione per l'adempimento all'obbligo di integrazione dell'informativa e della raccolta del consenso dall'interessato, nonché per la compresenza di una doppia finalità.

Proprio per superare tali elementi di ostacolo il sistema eTriage è stato progettato per l'utilizzo di dati anonimi nel suo interno.

L'anonimizzazione del dato avviene direttamente ad opera del *provider*, ovvero dell'organismo sanitario che acquisisce il dato e lo immette nel *database*, attraverso dei protocolli condivisi con tutti gli altri *provider* del sistema[46]. Successivamente, il flusso di dati dal *provider* al database centrale condiviso è generato mediante l'uso di informazioni totalmente anonime, sganciate da qualunque elemento identificativo.

Come si è detto, l'uso di dati anonimi consente di poter operare senza dover adempiere agli obblighi imposti dal Codice *Privacy*, non essendo più applicabile il concetto stesso di dato personale alle operazioni svolte e, conseguentemente, il trattamento non ricade nell'applicazione della normativa in materia di protezione dei dati personali[47].

[46] Un dato può ritenersi anonimo solo se la sua anonimizzazione è definitivamente irreversibile, ovvero l'interessato non può più essere identificato o identificabile. In tal senso, si veda il parere 1/2008 del Gruppo di Lavoro Articolo 29 in materia di protezione dei dati relativi ai meccanismi di ricerca.

[47] Cfr. nota n. 287, Cap. 11, par. 3

Da ciò ne consegue anche l'irrilevanza delle questioni, già ampiamente illustrate, circa l'inquadramento nei ruoli *privacy* dei soggetti coinvolti nell'architettura in *cloud* del progetto eTriage[48].

A seguito dell'anonimizzazione dei dati, in relazione all'informativa potrebbe porsi la questione se sia dovuta un'integrazione della stessa fornita al momento della raccolta del dato sanitario (in pratica l'informativa dei pazienti "storici") informando l'interessato del trattamento eseguito in ordine all'anonimizzazione dei dati conferiti. L'art. 13 del Codice *Privacy*, tuttavia, non prevede che nell'informativa siano elencati i trattamenti ma unicamente le finalità e le modalità. Pertanto, non è necessario procedere all'integrazione dell'informativa fornita ai pazienti storici.

Peraltro, il trattamento dei dati effetuato ai fini di anonimizzare gli stessi è un tipo di trattamento consentito dallo stesso Codice *Privacy*. Infatti, secondo l'art. 20 del Codice, i soggetti pubblici (come nel caso del progetto eTriage) possono trattare dati sensibili solo se autorizzati da una specifica disposizione di legge. Orbene, la disposizione di rango primario che autorizza l'organismo sanitario pubblico a procedere all'anonimizzazione è ricavabile dallo stesso art. 3 del Codice *Privacy* nella parte in cui dispone che "*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*". La disposizione qui riportata trova anche uno specifico richiamo all'art. 94 recante disposizioni in materia di trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario.

Alla luce di ciò, in tutti i casi in cui il trattamento dei dati sanitari avviene mediante l'impiego di sistemi informatici per finalità realizzabili attraverso dati anonimi, come nel progetto eTriage, la trasformazione in forma anonima rappresenta un vero e proprio obbligo di legge per tutti i titolari del trattamento.

[48] La tematica è stata oggetto di approfondimento nella parte quarta, al paragrafo 2.2 "Difficoltà di inquadramento soggettivo".

CONCLUSIONI

L'evoluzione normativa e tecnologica in corso non consente la formulazione di conclusioni nel senso più stretto del temine e all'esito della presente ricerca può affermarsi soltanto che la diffusione del *cloud computing*, nel comparto sanitario, per quanto già ben avviata, è ancora in fase di decollo.

In contesti trasversali, come quelli oggetto del presente studio, è una costante la complessità relazionale tra legislatori, giuristi, operatori sanitari, informatici e pazienti.

Il *cloud computing* ha, senza dubbio, il potenziale per rivoluzionare il modo in cui operano le aziende sanitarie (pubbliche e private), ma come spesso accade quando si adotta una nuova tecnologia, arrivano anche nuovi rischi e minacce, che devono essere attentamente compresi e analizzati, prima della migrazione. L'attività di ricerca confluita nel presente elaborato ha esplorato le aree del *cloud computing* nelle quali sono tuttora presenti minacce per la sicurezza. Prendendo spunto dai principi fondamentali dell'*information security,* e dalle linee guida proposte da alcuni organismi internazionali, si è mostrata la mappatura tra vulnerabilità e minaccia, che coinvolge gli ambiti della virtualizzazione e non solo, arrivando a classificare i rischi più elevati, che frenano la corsa verso la nuvola informatica, soprattutto nei settori, come quello sanitario, ove le vulnerabilità causano le più gravi conseguenze.

Permangono tutt'oggi, sul versante della sicurezza, numerose difficoltà che ancora devono essere affrontate e superate, perché il *cloud computing* possa essere adottato su larga scala. La prima è la mancanza di standardizzazione tra i servizi offerti dai *Cloud Provider* e le tecnologie impiegate (*hypervisor*, API, ecc), che non aiuta l'interoperabilità e la portabilità, favorendo il *lock-in*. Vi è, poi, l'ostacolo rappresentato dalla sicurezza, soprattutto derivante dai più noti attacchi alle reti tradizionali, come il DoS, in un ambiente virtualizzato. Inoltre, si rende necessario dover superare la condizione del fruitore del servizio *cloud* di perdita di controllo sui suoi dati, abbinata al rischio per la riservatezza e l'integrità.

Dall'analisi, in chiave giuridica, svolta nella fase successiva della ricerca, è risultato che la diffusione del *cloud computing*, fino ad oggi, è avvenuta con scarsa valutazione dell'impatto normativo, che, per quanto rappresenti un elemento esterno alla tecnologia, è capace di imbrigliarla e soffocarne lo sviluppo. Si pensi, in settori delicati come quello sanitario, alla progettazione di piattaforme deputate al trattamento di dati sensibili senza tenere in dovuta considerazione la disciplina dettata a tutela dei più elevati diritti della persona di rango costituzionale.

Ciò ha determinato il diffondersi di una prassi progettuale ed esecutiva volta alla realizzazione di soluzioni di tipo *cloud*, senza la minima (o con scarsissima) valutazione degli aspetti giuridici più rilevanti: la protezione dei dati personali (e spesso sensibili), la disciplina applicabile ai casi di *cloud* transnazionale (con ogni conseguenza in termini di tutela delle parti e giurisdizione competente) è l'inquadramento negoziale (finalizzato ad individuare i diritti e doveri delle parti) sono soltanto alcuni dei motivi che hanno generato diffidenza (rallentandone lo sviluppo) nei confronti dei servizi *cloud*.

Eppure anche il *trend* normativo di ultimissima generazione è orientato verso la scelta di soluzioni di *cloud computing*: si consideri a mero titolo d'esempio la folta disciplina dettata in materia di conservazione dei documenti digitali, la quale contempla espressamente l'esternalizzazione presso conservatori accreditati.

Soltanto con uno dei più recenti interventi del legislatore Europeo, peraltro giunto nella fase conclusiva della presente ricerca, è stato finalmente codificato il paradigma "*data protection by design and by default*" rafforzando la tutela dei diritti e delle libertà degli interessati fin dal momento della progettazione di ogni soluzione tecnologica che impatti con i diritti inviolabili della persona.

La progettazione e lo sviluppo *secundum legem* assume una particolare rilevanza nel contesto sanitario europeo, che già da qualche anno con la Direttiva 2011/24/UE dal 2011 aveva concretizzato il concetto di assistenza transfrontaliera, recepita in Italia con il Decreto legislativo 4 marzo 2014, n. 38.

In un momento storico di grande diffusione dei servizi di *cloud computing*, la codificazione del "*data protection by design and by default*" rappresenta una grande conquista anche se, per la sua piena operatività si

dovranno attendere ancora due anni, che in termini di sviluppo tecnologico sono un tempo immenso.

Le problematiche di natura negoziale, invece, sono tutt'altro che superate e forse destinate a espandersi, parallelamente alla crescente diffusione di servizi sempre più variegati e combinati.

I contratti di *cloud computing* patiscono le medesime, e datate, problematiche dei contratti informatici, che, nonostante i notevoli sforzi della dottrina e della giurisprudenza, continuano a diffondersi, nella prassi commerciale, in uno scenario tipico da "*far west*".

Le parti, spesso, nella definizione del regolamento contrattuale, trascurano aspetti fondamentali, quali ad esempio: le modalità di tenuta delle informazioni digitali in formato standardizzato per la migliore fruizione, i tempi e i modi di rilascio delle stesse, la migrazione ad altra piattaforma *cloud* gestita da altro *provider*, la legge applicabile in caso di *cloud* internazionale ecc.

Tutto questo genera una forte incertezza nella gestione dei rapporti di *cloud computing* e nella soluzione degli eventuali contenziosi tra *cloud provider* e fruitore del servizio, che si trasforma in un forte limite per la scelta di servizi di *cloud*.

D'altro canto, il consapevole e corretto uso dello strumento contrattuale può certamente diventare il volano per la rapida diffusione del *cloud computing*, anche per tutti gli aspetti non ancora disciplinati, come, ad esempio, quelli di natura tecnico-informatica. Il contratto, infatti, per espressa previsione normativa (art. 1372 c.c.) ha forza di legge tra le parti e quindi può supplire anche ad eventuali lacune di un singolo settore. Questa previsione, combinata con la libertà contrattuale di cui all'art. 1322 c.c. può diventare il punto di forza del *cloud computing*, per creare accordi solidi e sicuri volti ad incentivare la migrazione verso la nuvola computazionale.

BIBLIOGRAFIA

ABDELHAK M., *Health Information Management of a Strategic Resource*, W. B. Saunders Company, Philadelphia, 1996

ABETI R., *I nuovi contratti: nella prassi civile e commerciale*, 2004

AGUILAR L. J., *CLOUD COMPUTING - Notes for a spanish cloud computing strategy*, in Spanish Institute of Strategic Studies' Magazine, 2012

ALANAZI H. O., *Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance*, Journal of Medicinal Plants Research 2010, 4(19).

ALPA G., *I contratti di utilizzazione del* computer, in Giur. it 1983, IV.

ANDERSON J. G., *Security of the distributed electronic patient record: a case-based approach to identifying policy issues*, International Journal of Medical Informatics, 2000, 60.ANDERSON R. J., *Security in Clinical Information Systems*, University of Cambridge, 1996

ARMELLIN G., BETTI D., CASATI F., CHIASERA A., MARTINEZ G., STEVOVIC J., *Privacy preserving event driven integration for interoperating social and health systems*, Secure Data Management: 7th Vldb Workshop (SDM'10), September 2010.

ARNÒ G., *I contratti relativi all'*hardware, in I contratti, 1995.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 08/2012 providing further input on the data protection reform discussions*, WP199, 01574/12/EN, Brussel, 2012

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent*, adopted on 13 July, 201101197/11/EN, WP187

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Thirteenth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2009*, adopted on 14 July 2010, Brussels, 2011

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, adopted on 15 February 2007, 00323/07/EN, WP 131

ARTICOLO 29 GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI, *Parere 4/2007 sul concetto di dati personali*, adottato il 20 giugno, 01248/07/IT, WP 136

ATIENZA A. ET AL., *Critical Issues in eHealth Research*, Am J Prev Med, 2007, 32.

BADGER L., GRANCE T., PATT-CORNER R., VOAS J., "*Cloud computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology - NIST* " *Special Publication* 80-146, 2012

BAKER G.R., NORTON P., *Patient Safety and Healthcare Error in the Canadian Healthcare System. A Systematic Review and Analysis of Leading Practices on Canada with Reference to Key Initiatives Elsewhere. A Report to Health Canada*, Ottawa, Health Canada, 2002

BARNES D., SAKANDAR B., *Cisco LAN Switching Fundamentals*, Ciscopress, 2005.

BARRY R. ET AL., *Hype Cycle for Healthcare Provider Applications and Systems*, Report number G00127849, Stamford CT: Gartner Research, 2005

BARTOLI C., MEDAGLIA M., *Il riutilizzo dei dati nel settore della sanità pubblica: il progetto e-triage "*triage on the cloud*"*, CATTID, Università Sapienza di Roma

BASSI E., *PSI, protezione dei dati personali, anonimizzazione*, in "Informatica e diritto", ESI Italiane, Napoli, fasc. 1-2, 2011.

BATES D.W. ET AL., *The impact of computerized physician order entry on medication error prevention*, Journal of the American Medical Informatics Association", 1999, 6(4).

BATTELLI E., *Il nuovo Diritto europeo dei contratti nell'ambito della Strategia "Europa 2020"*, Contratti, 2011, XI.

BAZARGAN F., YEUN C. Y., ZEMERLY M. J., *State-of-the-Art of Virtualization, its Security Threats and Deployment Models*, in International Journal for Information Security Research (IJISR), vol. 2, (2012).

BELISARIO E., "Cloud Computing" , Informatica Giuridica – collana diretta da Michele Iaselli - eBook n.17, Altalex 2011

BENDANDI S., Software as a Service *(Saas): aspetti giuridici e negoziali*

BENNET C., TIMBRELL G. T., *Application Service Providers: Will They Succeed?*, in Information Systems Frontiers (ISF), vol. 2, n. 2, 2000.

BERNSTEIN K. ET AL., *Modelling and implementing electronic health records in Denmark*, International Journal of Medical Informatics, 2005, 74.

BIRNHACK M. D., *The EU Data Protection Directive: An engine of a global regime*, Computer Law&Security Report, 2008, 24.

BOLOGNINI L., D. FULCO, E. PELINO, *Dati sanitari e* Cloud Computing *per finalità di triage di pronto soccorso: profili e criticità in materia di protezione dei dati personali*, Istituto Italiano per la Privacy

BONAZZI E., TRIBERTI C., *Guida ai contratti dell'informatica*, 1990

BORKING J., RAAB C., *Laws, PETs and Other Technologies for Privacy Protection*, Refereed Article, 2001 (1), The Journal of Information, Law and Technology, 2001

BOS' J.J., *Digital signatures and the electronic health records: providing legal and security guarantees*, International Journal of Bio-Medical Computing, 1996.

BRADSHAW – MILLARD - WALDEN, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, 1 September 2010

BRAGGION A., *La validità delle clausole che limitano od escludono la responsabilità nei contratti per la fornitura di* software*: una rassegna di recenti pronunzie nella giurisprudenza europea*, Riv. dir. ind. 1989, I, 217

BRAVO F., *Appalti pubblici per la fornitura di beni e servizi nel settore ICT e tecniche di redazione contrattuale. Le linee guida del CNIPA*, in Dir. inf. e informatica, 2007.

BRIGHI R., VIRONE M.G., *Una tutela "by design" del diritto alla salute. Prospettive di armonizzazione giuridica e tecnologica*, in: *A Matter of Design: Making Society trough Science and Technology*, Milano, Open Access Digital Publication by STS Italia Publishing, 2014.

BROOKS T. T., CAICEDO C., PARK J. S., *Security Vulnerability Analysis in Virtualized Computing Environments*, in International Journal of Intelligent *Computing* Research (IJICR), 2012, vol. 3(1/2)

BROWN N., REYNOLDS M., *Strategy for production and maintenance of standards for interoperability within and between service departments and other healthcare domains*, Short Strategic Study CEN/TC251/N00-047, CEN/TC 251 Health Informatics, Brussels, Belgium, 2000

BUSCEMI A., CARRARO A., *L'innovazione tecnologica RFID a garanzia della sicurezza del paziente*, in "Diritto Sanitario Moderno", 2011, 59.

BUYYA R., RANJAN R., CALHEIROS R. N., *InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services*, in Algorithms and Architectures for Parallel Processing - Lecture Notes in *Computer* Science, 2010, vol. 6081.

CAGNASCO O., COTTINO G., *Contratti commerciali*, in *Trattato di Diritto Commerciale* diretto da G. COTTINO, Padova, 2000.

CANNON D.S., ALLEN S.N., *A comparison of the effects of computer and manual reminders on compliance with a mental health clinical practice guideline*, Journal of American Medical Information Association, 2000, 7.CARDARELLI F., *La cooperazione fra imprese nella gestione di risorse informatiche: aspetti giuridici del c.d.* outsourcing, in Dir. informaz. informat., 1993, I.

CARINGELLA F., BUFFONI L., Manuale di diritto civile - V Edizione, 2015

CARLIN S., CURRAN K., *Cloud Computing Security*, in International Journal of Ambient *Computing* and Intelligence, 2011, vol. 3(1).

CARLIN S., CURRAN K., *Cloud Computing Security*, International Journal of Ambient *Computing* and Intelligence, 3(1), 2011.

CARROL M., KOTZE'P., Van Der MERWE A., *Securing Virtual and Cloud Environments*, in *CloudComputing* and Services Science, Springer, 2012.

CAVOUKIAN A. (presentation by), *Privacy by Design: Building Trust into Technology*, 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research, Toronto, 2000

CAVOUKIAN A., ALVAREZ R. C., *Embedding Privacy into the Design of EHRs to Enable Multiple Functionalities - Win/Win*, Toronto, 2012.

CAVOUKIAN A., CHANLIAU M., *Privacy and Security by Design: A Convergence of Paradigms*, Toronto, 2013.

CAVOUKIAN A., EL EMAM K., *A Positive-Sum Paradigm in Action in the Health Sector*, Toronto, 2010.

CAVOUKIAN A., *Moving Forward From PETs to PETs Plus: The Time for Change is Now*, Toronto, 2009.

CAVOUKIAN, A., *Privacy by Design: Leadership, Methods, and Results*, 2013, in GUTWIRTH, S., LEENES, R., DE HERT, P. E POULLET, Y. (eds.), *European Data Protection: Coming of Age*, New York, Springer

CAVOUKIAN A., *Privacy by Design … Take the Challenge*, Toronto, 2009.

CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, Toronto, 2010.

CAVOUKIAN A., *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, in Yee G.O.M., Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, IGI Global, Hershey, 2012.

CAVOUKIAN, A., *Privacy by Design and the Promise of SmartData*, 2012, in HARVEY, I., CAVOUKIAN, A., TOMKO, G., BORRETT, D., KWAN, H. E HATZINAKOS, D. (eds.), *SmartData: Privacy Meets Evolutionary Robotics,* New York, Springer

CERINA P., *Contratti internazionali di informatica e Legge applicabile, prime considerazioni, in Dir. Infor e informatica,* 1994.

CHASE J., JAIPURIA P., *Managing Identity and Authorization for Community Clouds*, Technical Report CS-2012-08, Department of Computer Science, Duke University, 2012

CHING HSU I., *Extensible access control markup language integrated with Semantic Web technologies*, Information Sciences, 2013

CHRISTIAN W., MEINEL C., *Practical Network Security Teaching in an Online Virtual Laboratory*, in Proc. 2011 Intl. Conference on Security & Management , 2011, CSREA Press, Las Vegas, Nevada, USA

Cisco Systems, *Cisco Global Cloud Index: Forecast and Methodology, 2011–2016*, in *Global Cloud Index* (CGI), (2012)

CLOUD SECURITY ALLIANCE, *Security as a Service: Defined Categories of Service*, 2011

CODAGNONE C., LUPIÁÑEZ-VILLANUEVA F., *A composite index for the benchmarking of eHealth Deployment in European acute Hospitals. Distilling reality in manageable form for evidence based policy*, JRC Technical and Scientific Reports, Luxembourg: Publication Office of the European Union, 2011

COGO A., *Le regole del contratto tra* social network *e utente sull'uso della proprietà intellettuale del gestore, dell'utente e degli altri utenti – riflessioni a partire dall'individuazione del fenomeno, dei suoi soggetti e della funzione del contratto*, in AIDA, 2011.

COLLINGRIDGE D., *The Social Control of Technology*, St. Martin's Press, Frances Pinter, 1980

CONDE C. P., VILLANUEVA W. D., *Virtualization as a support for SOA and cloud computing*, in Aa.Vv. *Monograph: 2010 – Emerging Information*

Technologies (II), "The European Journal for the Informatics Professional" vol. XI, 2010.

CONKLIN WM. A., WHITE G., *Principles of Computer Security. CompTIA Security+TM and Beyond*, The United States of America, Mc Graw Hill, Second edition

CORASANITI G., *La sicurezza dei dati personali*, in Cardarelli, Sica, Zeno-Zencovich (a cura di), "Il codice dei dati personali. Temi e problemi", Giuffrè, Milano, 2004.

CSA, *Security guidance for critical areas of focus in cloud computing*, 2011 3°, (2009).

CURRAN K., CARLIN S., ADAMS M., *Security issues in cloud computing*, in Elixir Network Engg 38, (2011)

CURRIE W. L., *Towards a Healthier Europe!*, The TEMPEST Model, 2010

D.F. PARKHILL, *The Challenge of the Computer Utility*, Reading (Mass.), 1966

D'AGOSTINI D. ET AL., *La sicurezza delle informazioni in ambito sanitario*, in "Mondo Digitale", 2010, 2.

D'ARRIGO, *Prospettive della c.d. licenza a strappo nel nostro ordinamento*, in Dir. Inf., 1996.

DANZON P.M., FURUKAWA M., *e-Health: Effects of the Internet on Competition and Productivity in Health Care*, in Rivlin A. M., Liton R. E. (eds.), "The Economic Payoff from the Internet Revolution", Washington DC, The Brookings Task Force on the Internet, Brookings Institution Press, 2001

DAWOUD W., TAKOUNA I. , MEINEL C. , *Infrastructure as a service security: Challenges and solutions*, in Informatics and Systems (INFOS), 2010 The 7th International Conference, 2010.

D'COSTA-ALPHONSO M-M., MICHAEL M., *The adoption of single sign-on and multifactor authentication in organisations: a critical evaluation using TOE framework*, 2010, in Informing Science and Information Technology, vol. 7:161-190.

DE NOVA, Il contratto alieno, Torino, 2010

DEKKER M.A.C., ETALLE S., *Audit-Based Access Control for Electronic Health Records*, Electronic Notes in Theoretical Computer Science, 2007, 168.

DELLO IACOVO,L. Stampanti 3D, auto che si guidano da sole, intelligenza artificiale: ecco le 12 tecnologie che cambieranno il mondo, www.ilsole24ore.it, 24-5- 2013

DEMCHENKO Y., NGO C., DE LAAT C., GARCIA-ESPIN J., FIGUEROLA S., RODRIGUEZ J., CONTRERAS L., LANDI G., CIULLI N., *Intercloud Architecture Framework for Heterogeneous Cloud based Infrastructure Services Provisioning On-Demand*, 2013

DI COCCO C., *Soggetti che effettuano il trattamento (Parte I-Titolo IV)*, in J. Monducci, G. Sartor, "Il codice in materia di protezione dei dati personali", CEDAM, Padova, 2004.

DICK R., STEEN E. B., DETMER D. (eds.), *The Computer Based Patient Record: An Essential Technology for Health Care*, Institute of Medicine, National Academy Press, 1997.

DOBREV A. ET AL., *Interoperable eHealth is Worth it. Securing Benefits from Electronic Health Records and ePrescribing. Study Report 2010*, European Communities, Bonn/Brussels, 2010.

DOLIN R.H. ET AL., *HL7 Clinical Document Architecture, Release 2*, J Am Med Inform Assoc., 2006, 13(1).

DONALD G., *Arpanet*, in Wikipedia (2014)

E. BELISARIO, *"Cloud Computing", Informatica Giuridica – collana diretta da Michele Iaselli* - eBook n.17, Altalex 2011

E-BUSINESS W@TCH,.*ICT and e-business in Hospital Activities. ICT and e-business activity in 2006*, Sector Report No. 10 2006, Bonn: Empirica; Brussels: European Commission, 2006

EICHELBERG M. ET AL., *Electronic Health Record Standards - a brief overview, conference paper for Information Processing in the Service of Mankind and Health*, ITI 4th International Conference on Information and Communications Technology, 2006

EMPIRICA & WRC [WORK RESEARCH CENTRE], *ICT & Ageing – European study on Users, Markets and Technologies, Preliminary findings*, Interim report, Bonn: Empirica; Dublin: Work Research Centre, 2008

EMPIRICA, *European countries on their journey towards national eHealth infrastructures*, eHealth Strategies Report, 2011.

EMPIRICA, *ICT standards in the health sector: .*

ENISA, *Cloud Computing Benefits, risks and recommendations for information security*, rev. B, (2012)

ERA, *eHealth strategies and implementation in European countries*, EHealth ERA Report, Luxembourg, Office for Official Publications of the European Communities, 2007.

ERICSON J., *Health intelligence: An End to "Needless"*, Information Mangement, February 2012.

EYSENBACH G., *What is e-health?*, Journal of Medical Internet Research, 2001, 3(2):e20

FABIANO N., *I nuovi paradigmi della rete.* Distribueted computing, cloud computing e "computing paradigms":abstract *sugli aspetti e profili giuridici*

FALLETTI G., *Il contratto di* application service providing, in Il Dir .infor e informatica, 2001.

FENG J., CHEN Y., KU W., LIU P., *Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms*, in Parallel Processing Workshops (ICPPW), 2010 39th International Conference, 2010.

FERNÁNDEZ-ALEMÁN J. L. ET AL., *Security and privacy in electronic health records: A systematic literature review*, Journal of Biomedical Informatics, 2013

FINOCCHIARO G., *I contratti ad oggetto informatico*, 1993.

FLATLEY BRENNAN P. ET AL., *Project HealthDesign: Rethinking the power and potential of personal health records*, Journal of Biomedical Informatics, 2010, 43, S3-S5

FLICK C. - AMBRIOLA V., *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in Federalismi.it, 2013

FLORIO A., *Il trattamento dei "dati idonei a rivelare lo stato di salute" da parte dei medici liberi professionisti*, in "Ciberspazio e Diritto", 2010, vol. 11, n. 1.

FOSTER I., KESSELMAN C., *The Grid: Blueprint for a New Computing Infrastructure*, San Francisco, Morgan Kaufmann, 1999

GALGANO F., *La cultura giuridica italiana di fronte ai problemi informatici*, in G. Alpa, V. Zeno Zencovich, I contratti d'informatica, 1986.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*, Autorizzazione n. 2/2013, pubblicata in G.U. n. 302 del 27.12.2013,

valida dal 1° gennaio 2014 al 31 dicembre 2014, salve eventuali modifiche del Garante

GARETS D., DAVIS M., *Electronic Patient Records. EMRs and EHRs*, Healthcare Informatics, 2005

GARFINKEL S., *The Cloud Imperative*, in "*MIT Technology Review*", (2011)

GARTNER, *eHealth for a Healthier Europe! – opportunities for a better use of healthcare resources*, Västerås, Sweden: Edita, 2009

GLORIO D., *Il Cloud Computing nella P.A. e nei servizi demografici*, Lo Stato civile italiano, 2013

GOLDBERG I. ET AL., *Privacy-Enhancing Technologies for the Internet*, in "Proceedings of IEEE COMPCON '97", 1997.

GOLLMANN D., *Computer security*, in WIREs Computational Statistics, John Wiley & Sons, 2010, vol. 2:544-554.

GRITZALISA D., LAMBRINOUDAKIS C., *A security architecture for interconnecting health information systems*, International Journal of Medical Informatics, 2004, 73.

GUL I., UR REHMAN A., ISLAM M. H., *Cloud Computing Security Auditing*, in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference, 2011.

GÜRSES S. ET AL., *Engineering Privacy by Design*, in "Conference of Computers, Privacy & Data Protection", 2011.

HAAS S. ET AL., *Aspect of privacy for electronic health records*, International Journal of Medical Informatics, 2011, 80, e26-e31

HÄYRINEN K. ET AL., *Definition, structure, content, use and impacts of electronic health records: A review of the research literature*, International Journal of Medical Informatics, vol. 77, 2008.

HILLESTAD R. ET AL., *Can electronic medical record systems transform healthcare? Potential health benefits, savings, and costs*, Health Affairs, 2005, 24(5).

HOERBST A., AMMENWERTH E., *Quality and Certification of Electronic Health Records. An overview of current approaches from the US and Europe*, Applied Clinical Informatics, 2010.

HUANG L. ET AL., *Privacy preservation and information security protection for patients' portable electronic health records*, Computers in Biology and Medicine, 2009, 39.

HÜBNER U. ET AL., *ICT supporting nurses and physicians in hospitals: results of a comparative survey in Austria and Germany*, Studies in Health Technology and Informatics, 2009; 146:20-4

HÜBNER U. ET AL., *IT adoption of clinical information systems in Austrian and German hospitals: results of a comparative survey with a focus on nursing*, BMC Medical Informatics and Decision Making, 2010, 10:8 190

IAKOVIDIS I., *Towards Personal Health Record: Current situation, obstacles and trends in implementation of Electronic Healthcare Records in Europe*, International Journal of Medical Informatics, 1998, 52, 128.

IASELLI M., *I contratti informatici (III edizione)*, Altalex 2015

IDABC, EIF, *European Interoperability Framework for Pan-europeaneGovernment Services*, v. 1.0, Brussel, 2004.

INFORMATION ASSURANCE TECHNOLOGY ANALYSIS CENTER (IATAC), *Data and Analysis Center for Software* (DACS), *Software Security Assurance*, in State of-the-Art Report (SOAR), 2007.

IVONE V., *Commento all'art. 1766*, in Dei singoli contratti, vol. II, in Commentario al Cod. Civ. diretto da E. Gabrielli, 2011.

IZZO U., GUARDA P., *Sanità elettronica, tutela dei dati personali e digital divide generazionale. Ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, Trento Law and Technology Research Group, ResearchPaper Series n. 3, 2010,

JAEGER P. T., LIN J., GRIMES J. M., *Cloud Computing and Information Policy: Computing in a Policy Cloud?* In Forthcoming in the Journal of Information Technology and Politics, 2008, vol. 5(3):269-283

JAEGER P. T., LIN J., GRIMES J. M., SIMMONS S. N., *Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing*, in First Monday, 2009, vol. 14(5)

JITHIN P., JAYAKUMAR S. K. V., *Performance comparison of web service in IaaS cloud and standard deployment model*, in International Journal of *Computer* Trends and Technology (IJCTT), 2013, vol. 4(6.

JØSANG A., FABRE J., HAY B., DALZIEL J., POPE S., *Trust requirements in identity*

KANDUKURI B., PATURI R., RAKSHIT A., *Cloud Security Issues*, in IEEE International Conference on Services *Computing*, (2009)

KARLA D., *Electronic Health Records Standards*, IMIA Year Book of Medical Informatics, 2006.

KHAN K. M., MALLUHI Q., *Establishing Trust in Cloud Computing*, in IT Professional , 2010, vol. 12(5).

KHARCHE H., CHOUHAN D. S., *Building Trust in Cloud Using Public Key Infrastructure*, in International Journal of Advanced *Computer* Science and Applications, 2012, vol. 3(3).

KHARRAZI H. ET AL., *Mobile personal health records: An evaluation of features and functionality*, International Journal of Medical Informatics, Vol. 81, Issue 9, 2012.

KO M. N., CHEEK G. P., SHEHAB M., SANDHU R., *Social-networks connect services*, in *Computer*, 2010, vol. 43(8).

KPMG, *The cloud takes shape. Global cloud survey: the implementation challenge*, (2013).

KREIZMAN G., ROBERTSON B., Incorporating Security into the Enterprise Architecture Process, Gartner, 2006

KREPS G. L., NEUHAUSER L., *New directions in eHealth communication: Opportunities and challenges,* Patient Education and Counseling, 2010, 78.

KUM H.C., AHALT S., *Privacy-by-Design: Understanding Data Access Models for Secondary Data*, AMIA Summits TranslSci Proc., 2013.

LEONE S., *La concessione del software tra licenza e locazione*, in G. Alpa, V. Zeno Zencovich, I contratti d'informatica, 1986.

LICKLIDER J.C.R., *Memorandum For Members and Affiliates of the Intergalactic Computer Network*

LISI A. - UNGARO S., *Cloud & PA: nuovi profili di responsabilità*, in Guida al pubblico impiego, 2012

LISI A. - UNGARO S., *Cloud e PA: sarà più facile andare 'sulle nuvole'*, in Guida al pubblico impiego, 2013

LISI A. - UNGARO S., *Cloud: vanno indicati ruoli e responsabilità*, in Guida al pubblico impiego, 2012

LONDON ECONOMICS, *Study on the economic benefits of privacy-enhancing technologies (PETs)*, Final Report to The European Commission DG Justice, Freedom and Security, London, 2010.

LONDON ECONOMICS, *Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security*, London, 2010,

MAGGI M., *Il contratto di fornitura di sistema informatico come contratto indeterminato*, nota a Cass. Sez. II, 22 marzo 1999, n. 2661, in I Contratti, 1999.

MALIK A., NAZIR M. M., *Security Framework for CloudComputing Environment: A Review*, in Journal of Emerging Trends in *Computing* and Information Sciences, vol.3, n. 3, (2012).

MALIN B. AT AL., *Biomedical data privacy: problems, perspectives, and recent advances*, J Am Med Inform Assoc, 2013, 20.

MALIN B. ET AL., *Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research*, J Investig Med., 2010, 58(1).

MALIN B., ET AL., *Learning relational policies from electronic health record access logs*, Journal of Biomedical Informatics, 2011, 44.

management, in Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44, pp. 99-108

MANCARELLA M., "E-health *e diritti, l'apporto dell'informatica giuridica*, 2012

MANTELERO A., *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. Informaz.informat., 2010.

MANTELERO A., *"Processi di Outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali" Saggi*, in Dir. Informaz.informat., 2010

MANTELERO A., *Il contratto per l'erogazione dei servizi di* cloud computing, in Contratto e Impresa 4-5/2012 .

MANTELERO A., *Processi di* Outsourcing *informatico e* cloud computing*: la gestione dei dati personali ed aziendali* Saggi, in Dir. Informaz.informat., 2010.

MARTIN D., SERJANTOV A. (edited by), *Privacy Enhancing Technologies, Proceeding of 4° international workshop PET 2004*, Toronto - Berlin, 2004

MATHEW A., *Security and privacy issues of cloud computing; solutions and secure framework*, in International Journal of Multidisciplinary Research, 2012, vol. 2(4).

MELL P., GRANCE T., *The NIST Definition of Cloud Computing: Recommendation of the National Institute of Standards and Technology*, NITS, US Department of Commerce, Gaithersburg (MD)2011

MICHAEL B., DINOLT G., *Establishing Trust in Cloud Computing*, in IA-Newsletter, 2010, vol. 13(2).

MINISTERO DELLA SALUTE, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, Roma, 2010, pp. 28

MOEREL L., *Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof*, Tilburg University, 2014.

MORGAN R. L., CANTOR S., CARMODY S., HOEHN W., KLINGENSTEIN K., *Federated Security: The Shibboleth Approach*, 2004, in EDUCAUSE Quarterly, vol. 27(4).

MORUZZI M., *e-Health e Fascicolo Sanitario Elettronico*, Il Sole 24 Ore, 2009.

MUSELLA A., *Il contratto di* outsourcing *del sistema informativo*, in Dir. informaz. informat., 1998.

NATIONAL INSTITUTES OF HEALTH - NATIONAL CENTER FOR RESEARCH RESOURCES, *Electronic Health Record Overview*, MITRE Center for Enterprise, McLean, Virginia, 2006 .

NELSON M.R., *Building an Open Cloud, Science*, 26-6-2009, 1656;

NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, in Special Publication 800-144, 2011

NIST, *NIST Cloud Computing Reference Architecture*, in *Special Publication* 500-292, 2011

NORDIC COUNCIL OF MINISTERS, *Health and Social Sectors with an "e". A study of the Nordic countries*, 2005, Copenhagen .

OECD HEALTH POLICY STUDIES, *Improving Health Sector Efficiency. The Role of Information and Communication Technologies*, 2010

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY - COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, *Working Party on Information Security and Privacy. Inventory of Privacy-Enhancing Technologies (PETs)*, DSTI/ICCP/REG(2001)1/FINAL, 2002.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Improving Health Sector Efficiency: The Role of Information and*

Communication Technologies, OECD Health Policy Studies. Paris: OECD Publishing, 2010.

OSNAGHI A., *Pubblica amministrazione che si trasforma: «Cloud Computing», federalismo, interoperabilità*, in Amministrare, 2013

PAGALLO U., BASSI E., *The Future of EU Working Parties' "The Future of Privacy" and the Principle of Privacy by Design*, in M. Bottis (eds.), "An Information Law for the 21st Century", Atene, NomikiBibliothiki, 2011.

PAGALLO U., *Designing Data Protection Safeguards Ethically*, in Information, 2011, 2.

PAGALLO U., *On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law*, in S. Gutwirth et al. (eds.), "European Data Protection: In Good Health?", Springer Science+Business Media B.V, 2012.

PAGALLO U., *Privacy e Design*, in M. Pietrangelo (a cura di), "Diritti di libertà nel mondo virtuale della rete", Informatica e diritto, 2009, 1.

PAGLIARI C. ET AL., *Potential of electronic personal health records*, British Medical Journal, 2007.

PAHL C., ZHANG LI, FOWLEY F., *A Look at Cloud Architecture Interoperability through Standards*, in CLOUD COMPUTING 2013, The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization, 2013.

PAL S., KHATUA S., CHAKI N., SANYAL S., *A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security*, in Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research Article No. 76, 2011.

PATHAK J. ET AL., *Applying linked data principles to represent patient's electronic health records at Mayo clinic: a case report*, in "Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium", ACM New York, USA, 2012.

PERRI P., *Introduzione alla sicurezza informatica e giuridica*, in Pattaro E. (a cura di), "Manuale di diritto dell'informatica e delle nuove tecnologie", Cluebs.c.a.r.l., Bologna, 2002.

PERRI P., *Le misure di sicurezza*, in Monducci J., Sartor G., "Il codice in materia di protezione dei dati personali", CEDAM, Padova, 2004.

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007.

PHAM Q., MCCULLAGH A., DAWSON E., *Consistency of user attribute in federated systems,*in Trust, *Privacy* and Security in Digital Business , 2007.

PHAPHOOM N., WANG X., ABRAHAMSSON P., *Foundations and Technological Landscape of Cloud Computing*, in ISRN Software Engineering, 2013, Article ID 782174

PIANA C., *Licenze pubbliche di* software *e contratto*, in I Contratti, 2006.

PITTALIS M., Outsourcing, *in Contratto e Impresa*, 2000, pp. 1010 ss.

PÒ M., *Dal Cloud computing nuove opportunità per la Sanità*, in Guida al pubblico impiego, 2012

PRIVACY ENHANCING TECHNOLOGIES, *Proceeding of 4° international workshop, PET 2004*, Toronto, May 2004, Berlin, 2004

PROSPERETTI E., *L'opera digitale tra regole e mercato*, 2013

PROSPERETTI E., *La condivisione* one-click *di dati di terzi verso piattaforme Internet e le regole della* privacy, in Rivista di Diritto, Economia e Tecnologie della Privacy, 1, 2013.

QAISAR S., K. KHAWAJA F., *Cloud Computing: Network/Security Threats And Countermeasures*, In Interdisciplinary Journal Of Contemporary Research In Business, 2012, Vol. 3(9

Q-REC, WP3, *Inventory of Relevant Standards for EHR Systems*, v. 0.8, 2007.

RABAZZI C. ET AL., *La sicurezza informatica e la Privacy*, in G. Ziccardi (a cura di), "Telematica giuridica. Utilizzo avanzato delle nuove tecnologie da parte del professionista del diritto", Giuffrè, Milano, 2005, pp. 516 e ss.

RABBITO C., *Sanità elettronica e diritto. Problemi e prospettive*, Società Editrice Universo, 2010.

RIFKIN J., *L'era dell'accesso*, Milano, 2000

RODOTÀ S., *Privacy e costruzione della sfera privata (1991)*, in Id., "Tecnologie e diritti", Bologna, Il Mulino, 1995.

ROSENTHAL J., RILEY T., *Patient safety and medical errors: a roadmap for state action*, National Academy for State Health Policy, 2001

ROSSELLO C., *I contratti dell'informatica nella nuova disciplina del* software, 1997

ROSSELLO C., *La responsabilità da inadeguato funzionamento di programmi per elaboratori elettronici. Aspetti e problemi dell'esperienza nord americana*, in Riv. crit. dir. priv., 1984

ROSSI MORI A. ET AL. (a cura di), *Un quadro di riferimento sulle tecnologie dell'informazione nel settore sanitario*, Consiglio Nazionale delle Ricerche - Istituto Tecnologie Biomediche, 2003.

ROVERSI R., *I contratti di* outsourcing *della manutenzione*, in I Contratti, 1997.

SABOOWALA H., ABID M., MODALI S., *Design Network and Services for the Cloud*, Ciscopress, 2013.

SADAN B., *Patient data confidentiality and patient rights*, International Journal of Medical Informatics, 2001, 62.

SAMMARCO P., *Appalto di* software *e trasferimento di diritti*, in Giustizia civile, 1998.

SANDHU R. ET AL., *The NIST Model for Role-Based Access Control: Towards A Unified Standard*, Proceedings of the fifth ACM workshop on Role-based access control, 2000.

SANDHU R. S. ET AL., *Role-Based Access Control Models*, IEEE Computer, 1996, 29 (2).

SANJITHA D.V., HIMASWANTHI M., SAI SINDHURA T.V.N., SATYANARAYANA K.V.V., *Dependable and Secure Storage Services in Cloud Computing*, in International Journal of *Computer* Trends and Technology (IJCTT), 2013, vol. 4(4)

SCHAAR P., *Privacy by Design*, Identity in Information Society, 2010, 3, pp. 267-274 195

SCHULZ G., *Cloud and Virtual Data Storage Networking*, CRC Press, 2012.

SCUFFI M., I *Contratti per la manutenzione: verso il "*global service*"*, in Il Diritto Industriale, 1996.

SEONGHAN S., KAZUKUNI K., *Towards Secure Cloud Storage*, in Demo for CloudCom2010, (2010).

SICA S. E STANZIONE P. (a cura di), *La nuova disciplina della privacy, Commento al D.lgs. 30 giugno 2003, n. 196*, Bologna, 2005

SINGHAL P., *Data Security Models in Cloud Computing*, International Journal of Scientific & Engineering Research, 2013, vol. 4(6).

SITTIG D. F., *Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century*, International Journal of Medical Informatics, 2002, 65, 1–6

SMITH E., ELOFF J.H.P., *Security in health-care information systems-current trends*, International Journal of Medical Informatics, 1999, 54.

SMOOT S. R., TAN N. K., *Private Cloud Computing*, Morgan Kaufmann, 2012.

STALLMAN R., *Cloud computing is a trap*, in theguardian.com, 29-9-2008

STRANDBERG M., KRASNIK A., *Does a public single payer system deliver integrated care? A national survey among professional stakeholders in Denmark*, International Journal of Integrated Care, 2008.

STROETMANN K. A. ET AL., *eHealth in Action. Good Practice in European Countries. Good eHealth Report*, Luxemburg, 2009.

STROETMANN K. A. ET AL., *eHealth is worth it. The economic benefits of implemented eHealth solutions at ten European sites*, Luxembourg, Office of Official Publications of the European Communities, 2006

STROETMANN K. A. ET AL., *European countries on their journey towards national eHealth infrastructures. eHealth Strategies Report*, Bruxelles, 2011.

STROETMANN K. A., STROETMANN V. N., *Electronic business in the health and social services sector*, Sector Impact Study No. 10-I (draft), The European e-business W@tch 2003/4, Commissione europea, Direzione generale Imprese: Bruxelles/Bonn, 2004

SUMMERFIELD B., EMPEY E., *Computer-based Information Systems for Medicine: A Survey and Brief Discussion of Current Projects*, Santa Monica, Calif.: Systems Development Corporation, 1965

TANG P. C., ET AL., *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, Journal of the American Medical Informatics Association, 2006, 13 (2).

TETTERO O., *Intrinsic Information Security: Embedding Security Issues in the Design Process of Telematics Systems*, Technical Report 6, Telematica Instituut, Enschede, The Netherlands, 2000.

THOMAS I., MEINEL C., *An Identity Provider to manage Reliable Digital Identities for SOA and the Web*, in IDTRUST '10 Proceedings of the 9th Symposium on Identity and Trust on the Internet, 2010.

TOMOYOSHI T., TSUDA H., HASEBE T., MASUOKA R., *Data loss prevention technologies*, in Fujitsu Scientific and Technical Journal , 2010, vol. 46(1).

TOSI E., *Brevi note a margine del problema della qualificazione e dell'inadempimento del contratto di fornitura di* hardware *e* software, nota a Tribunale di Bari, 4 giugno 1994, in Il Dir. infor. e informatica, 1995.

TOSI E., *I contratti di informatica*, Il Sole 24 Ore, 1993

TOSI E., *Natura e qualificazione dei contratti di fornitura dei sistemi informatici*, nota a Tribunale Torino, 13 marzo 1993, in Dir. Infor. e informatica, 1995.

TOSI F., *Il contratto di* outsourcing *di sistema informatico*, Milano, 2001

TSAI C., STARREN J., *Patient Participation in Electronic Medical Records*, Journal of the American Medical Association, 2001, 285 (13).

UECKERT F. ET AL., *Empowerment of patients and communication with health care professionals through an electronic health record*, International Journal of Medical Informatics, 2003 70 (2-3), pp. 99-108

VAN BLARKOM RE G.W., BORKING J.J., OLK J.G.E. (eds.), *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*, PISA Consortium, The Hague, 2003.

VAN DER SLOOT B., *Public Sector Information & Data Protection: A Plea for Personal Privacy Settings for the Re-use of PSI*, in "Informatica e diritto", ESI, Napoli, fasc. 1-2, 2011.

VAN DEURSEN A. J.A.M., *Internet skill-related problems in accessing online health information*, International Journal of Medical Informatics, 2012, 81.

VAQUERO L. M., RODERO-MERINO L., CACERES J., LINDNER M., *ACM Computer Communication Review* , in "*A Break in the Clouds: Towards a Cloud Definition*", vol. 39, n. 1, gennaio 2009

VICENTE M. R., LÓPEZ A. J., *Assessing the regional digital divide across the European Union-27*, Telecommunications Policy, 2011, 35, pp. 220-237

VIOLA DE AZEVEDO M. ET AL., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, Ciberspazio e diritto 2010, 11.

WAEGEMANN P., *Status Report 2002: Electronic Health Records*, Medical Records Institute, 2002 197

WANG Z., LEE R. B., *Covert and Side Channels due to Processor Architecture*, in Proceedings of the 22nd Annual *Computer* Security Applications Conference, 2006 .

WARREN S., BRANDEIS L., *The Right to Privacy*, in Harvard Law Review, 1890, 4.

WARSCHOFSKY R., MENZEL M., MEINEL C., *Automated Security Service Orchestration for the Identity Management in Web Service based Systems,* in Web Services (ICWS), 2011 IEEE International Conference , 2011.

WILSON P. ET AL., *Mapping the Potential of eHealth. Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration 2004,

WINDLEY P. J., *Digital Identity,* O'Reilly Media, Inc, 2008.

XU Y., BAILEY M., JAHANIAN F., JOSHI K., HILTUNEN M., SCHLICHTING R., *An Exploration of L2 Cache Covert Channels in Virtualized Environments*, in Proceedings of the 3rd ACM workshop on *Cloud-computing* security workshop, 2011.

YI WEI, BLAKE M. B., *Service-Oriented Computing and Cloud Computing - Challenges and Opportunities*, in Internet *Computing*, IEEE, 2010, vol. 14(6).

YOUNGE A. J., HENSCHEL R., BROWN J. T., VON LASZEWSKI G., QIU J., FOX G. C., Analysis of Virtualization Technologies for High Performance Computing Environments, in Aa.Vv., IEEE 4th International Conference on Cloud Computing, (2011)

ZACCARIA A., *La responsabilità del produttore di* software, in Contratto e impresa, 1993.

ZHAO G., LIUJ J., TANG Y., SUN W., ZHANG F., YE X., TANG N., *Cloud Computing: A Statistics Aspect of Users*, In First International Conference on *Cloud Computing* (*Cloud*Com), Beijing, China, Heidelberg Springer Berlin, (2009).

ZHIXIONG C., YOON J. , *IT Auditing to Assure a Secure Cloud Computing*, in Services (SERVICES-1), 2010 6th World Congress, 2010.