diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 26/07/2012

All'indirizzo http://www.diritto.it/docs/33809-nuove-applicazioni-informatiche-ido-e-cloud-computing-nuovi-problemi-per-la-sicurezza-la-privacy-l-ambiente-ed-il-diritto

Autore: Sarzana Carlo di S.Ippolito

Nuove applicazioni informatiche: ido e cloud computing- nuovi problemi per la sicurezza, la privacy, l'ambiente ed il diritto

NUOVE APPLICAZIONI INFORMATICHE :IdO e CLOUD COMPUTING-NUOVI PROBLEMI PER LA SICUREZZA, LA PRIVACY, L'AMBIENTE ED IL DIRITTO. (*)

-

INTRODUZIONE

In relazione al dibattito in corso in vari paesi per quanto riguarda gli effetti ed i rischi di Internet nei vari settori della vita sociale ,ed in considerazione dei continui sviluppi della tecnologia informatica e della loro incidenza nell'ambito della sicurezza informatica, della protezione dei dati, della tutela dell'ambiente e dello stesso diritto, intendo qui esaminare succintamente alcuni riflessi dell'uso di recenti applicazioni informatiche, quali il cosiddetto *Internet degli oggetti* (IdO) ed il *cloud computing.* (il c.d computer nella "nuvola")[1].

* Il presente articolo riprende e sviluppa, con notevoli aggiunte ed integrazioni, alcuni *items* della mia introduzione al Convegno "Nuove tendenze della giustizia penale di fronte alla criminalità informatica", tenutosi a Como nel maggio del 2010 ,ed i cui atti sono stati pubblicati nell'anno successivo in un *e-book* dell'Editore Giappichelli.

1 Colgo l'occasione per ripetere qui una opinione che da molto tempo vado sostenendo in varie sedi, e da ultimo anche al Convegno di Como, e cioè che in un settore quale quello informatico nel quale le nuove tecnologie irrompono, creando necessità, a volte urgenti, di un inquadramento dei fenomeni nel campo del diritto, è divenuto difficile stare realmente al passo con la situazione giacché occorrono doti di costante attenzione,,di capacita , di osservazione delle nuove realtà, attenzione e capacità che devono essere accompagnate, ai fini di una comprensione e di un esatto inquadramento del fenomeno complesso, da una sensibilità , insieme, giuridica, sociologica e criminologica.

1) L' IdO E LE INIZIATIVE AL RIGUARDO DELLA COMMISSIONE CEE E DEL PARLAMENTO EUROPEO.LE INIZIATIVE LEGISLATIVE ITALIANE Ciò premesso, iniziando dal primo argomento , e cioè dall' **IdO**, rilevo anzitutto che da qualche tempo la pubblicistica specializzata, i legislatori di vari Paesi del mondo ed alcune organizzazioni internazionali, si stanno occupando delle conseguenze tecniche, giuridiche e sociali derivanti dallo sviluppo del cosiddetto *"INTERNET degli oggetti"* (**IdO**) chiamato anche "Informatica ubiquitaria" o "Intelligenza ambientale", con riferimento a determinate tecnologie *(R.F.I.D., TCP/IT, BLUETOOTH, ecc.),* che, collegate insieme, consentono di identificare oggettiraccogliere dati, trattarli e trasferirli.

L'Internet degli oggetti rappresenta una autentica rivoluzione tecnologica: in realtà esso costituisce il futuro del *computing* e delle stesse comunicazioni tradizionali, in virtù dello sviluppo di nuove tecnologie che vanno dai sensori wireless alle nanotecnologie.

Predomina in questo settore la tecnologia RFDI che consente, tra l'altro l'impianto dei *tags* nel corpo umano per scopi medici e favorisce, in modo notevolissimo, il commercio e le applicazioni commerciali specifiche.

Già in occasione della Conferenza Europea dal titolo *"INTERNET del futuro"*, tenutasi nell'ottobre del 2008, durante il *Summit* di Nizza dei Ministri dell'Unione Europea che si occupano dei problemi della società dell'informazione, è emersa la preoccupazione di vedere crescere i problemi relativi alla *"governance"* europea delle

infrastrutture relative all'**IdO** e si è prospettata la possibilità di attuare, tra l'altro, il c.d. *silenzio dei chips*.

L'argomento è stato oggetto ,di recente, di un'importante comunicazione della Commissione U.E. al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale, del 18 giugno 2009, dal titolo *L'INTERNET degli oggetti: un piano di azione per l'Europa* (COM/2009/278 fin.). La Commissione ha rilevato che l'*Internet degli oggetti* è composto da una serie di nuovi settori integrati che operano con infrastrutture proprie e che poggiano, in parte, sulle infrastrutture Internet esistenti, precisando che l'**IdO** può essere messa in relazione con nuovi servizi e riguarda tre modi principali di comunicazione che possono essere stabiliti in ambienti ristretti *(Intranet degli oggetti)* o pubblicamente accessibili *(Internet degli oggetti)* e cioè comunicazioni: a) da oggetto a persona; b) da oggetto ad oggetto; c) da macchina a macchina (M2M).

La Commissione ha precisato, poi, che l'**IdO** attualmente riguarda applicazioni quali:

- telefoni cellulari con accesso a internet, dotati di macchina fotografica;
- numeri di serie unici sui prodotti farmaceutici (in forma di codici a barre);
- sistemi intelligenti di misurazione dell'elettricità per fornire ai consumatori informazioni in tempo reale sui consumi;
- "oggetti intelligenti" nel settore della logistica (eFreight), nel settore manifatturiero o nella distribuzione commerciale.

La Commissione non ha potuto fare a meno di rilevare che la realizzazione della connessione degli oggetti solleva particolari questioni, quali, ad es. , l'identificazione dell'oggetto, l'autorità responsabile dell'attribuzione dell'identificatore, i mezzi per rilevare le informazioni relative all'oggetto, la garanzia della sicurezza delle informazioni, il quadro etico e normativo dell'internet degli oggetti, i meccanismi del controllo, ecc. In argomento la Commissione ha sottolineato che lo sviluppo dell'**IdO** deve rispettare la vita privata e la protezione dei dati personali[2]. Per tutelare la sicurezza delle informazioni, la Commissione ha, infine, chiesto agli Stati di rafforzare la sorveglianza e la protezione delle infrastrutture critiche informatiche[3]. Va detto ora che una delle più importanti realizzazioni dell'**IdO** è rappresentata dalla tecnologia R.F.I.D. (le c.d. *targhette intelligenti*): si tratta di sistemi che utilizzano le onde radio per la identificazione di oggetti, cose, animali e persone, utilizzando la

2 Ovviamente è possibile parlare di *privacy* solo se i dati trasmessi sono legati ad una persona fisica. Ha osservato un autore (N. FABIANO, *Internet of Things: il fenomeno e le prospettive giuridiche*, nel volume collettaneo Next Privacy,Milano, 2011….) che oltre alla possibilità di furti di identità allorché in qualche modo i dati sottratti possano essere tali da riguardare una persona fisica, esiste la circostanza che il soggetto interessato ignori addirittura il fatto che i vari dati che ai suoi oggetti si riferiscono, di per sé slegati, siano stati in qualche modo collegati, raccolti e contenuti in un *server* del quale il soggetto ignori perfino l'esistenza. In riferimento alla protezione dei dati personali l'autore osserva … *"questi, sebbene precedentemente memorizzati utilizzando un sistema che garantisce l'anonimato, qualora siano collegati ad altre informazioni o ai dati che riguardano il profilo tipico di una persona potrebbero presentare il rischio di essere rivelati: di conseguenza si potrebbe identificare una persona con le sue caratteristiche biometriche".*

3 A proposito dell'IdO un autore francese, MARC-OLIVIER PADIS, in un articolo dal titolo *Homo numericus – L'Internet et le nouveau outil informatique,* ha esaminato le conseguenze di quello che lui chiama *"La dispersion dell'Internet hors de sa sphere d'origine"* e, tra l'altro, ha osservato che *"... il ne s'agira plus alors de dérober un peu de notre tempe réel pour aller vivre dans le monde de simulation ou de compenser originariement une réalité décevant dans des mondes parallèles mais de vivre dans une "réalité augumentée".*

lettura a distanza dei *chips* da parte di appositi strumenti di lettura. In tal modo vengono catturate, per così dire, le *informazioni contenute* in una particolare etichetta. Il *tag R.F.I.D.* è tipicamente composto da un *micro chips* e da una antenna: in certi casi anche da una batteria.

La tecnologia R.F.I.D. è stata oggetto di una recente importante Comunicazione della Commissione U.E. (2009/387/CE) del 12 marzo 2009 che tratta, tra l'altro, dell'argomento relativo alla messa in opera dei principi relativi al rispetto della vita privata ed alla protezione dei dati nelle applicazioni relative all'identificazione mediante radiofrequenza, nella quale si afferma *(considerando n. 20)* che nel settore del commercio al dettaglio una valutazione degli impatti sulla protezione della vita privata e dei dati personali, dei prodotti contenenti etichette vendute ai consumatori dovrebbe fornire le necessarie informazioni per eliminare eventuali minacce alla stessa vita privata o alla protezione dei dati personali. A questo riguardo la Commissione ha emanato apposite raccomandazioni[4].

4 Recita in proposito il documento:"… *Au moyen d'un signe européen commun élaboré par des organismes européens de normalisation avec l'aide des parties concernées, les exploitants doivent informer les personnes de la presence d'Ètiquettes placées sur le produits ou incorporées à ceux-ci.*
Lors de la realisation de l'évaluation d'impact sur la protection des donne et de la vie privée visée aux points 4 e 5, l'exploitant d'application doit determiner précisément si les etiquettes placées sur des produits ou incorporées à des produits vendus aux consommateurs par des détaillantes qui ne sont pas exploitants de cette application presentment un risqué probable pour la vie privée ou la protection des donne à caractère personnel.
Les déteaillants doivent désactiver ou retirer, au point de vente, les etiquettes de leur application à moins que les, consommateurs, après avoir pris connaissance de la politique d'information visée au point, acceptant que les etiquettes restent opérationnelles. Par désactivation des etiquettes, on entend tout processus qui interrompt les interaction d'une etiquette avec son environnement et qui n'exige pas de participation active du consommateur. La désactivation ou le retrait des etiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateur doivent pouvoir verifier que la désactivation ou le retrait sont effectifs.
Le point 11 ne s'applique pas s'il resort de l'évaluation d'impact sur la protection des données et de la vie privée que les etiquettes utilisées dans une application de detail et restant opérationnelles au-delà du point de vente ne presentment pas de risqué probable pour la vie privée ou la protection des données à caractère personnel. Néanmois, les détaillants doivent metre gratuitement à disposition un moyen aisé de désactiver ou de retirer, immédiatement ou ultérieurement, ces etiquettes.
La désactivation ou le retrait des etiquettes ne doit impliquer aucune reduction ni cessation des obligations légales du détaillant ou de fabricant envers le consommateur.
Le points 11 e 12 ne s'appliquent quaux détaillants qui sont exploitants.

L'ENISA, e cioè l'Agenzia Europea per la Sicurezza delle Reti e dell'Informazione, ha recentemente analizzato i rischi associati allo scenario futuro dello sviluppo dell'IdO con particolari riferimenti ai viaggi aerei[5], formulando raccomandazioni apposite per quanto riguardava la *policy*, la ricerca e gli aspetti legali connessi.

I più importanti rischi enunciati nel *paper* riguardavano:

a) failure of reservation, check-in and trading procedures;

b) problems in issuing/enabling electronic visas;

c) loss/violation of citizen/passenger privacy;

d) compliance and abuse of state-owned citizen/passenger database;

e) repurposing of data/mission/crep;

f) Health processes-related concerns;

g) user frustration and low user acceptance;

h) aggressive profiling and social sorting leading to social exclusion;

i) legislation lagging behind rapid technological advancement;

l) non-compliance with date protection legislation.

Anche la stampa di larga diffusione ha iniziato ad occuparsi dell'argomento, prospettando i pericoli che l'internet degli oggetti potrebbe creare per la *privacy* (vedi l'articolo di A. Aquario dal titolo *"Macchine-Parla con loro. Dalla caffettiera al cruscotto"*, in La Repubblica del 3/4/2012).

5 Flyng 2.0 –*Enabling automated air travel by identifing and addressing the challenges of IoT and R.F.I.P technology,* aprile 2010.

Devo ricordare a questo punto per inciso che, già moltissimi anni fa, nei miei primi scritti ed interventi[6], avevo accennato ai profili di vulnerabilità della società informatizzata ed in particolare ai possibili attentati ai sistemi *"life support"*, o di diagnosi elettronica ed ai possibili errori nella gestione della relativa strumentazione[4]. In realtà lo sviluppo dei sistemi in questione ha accresciuto i problemi di sicurezza dei sistemi informatici, già notevoli a causa dei *virus* e degli *worms*, in quanto gli attacchi o i malfunzionamenti derivanti da errori o negligenze possono riguardare processi vitali per gli interessati giacché per molti pazienti, come ad esempio i cardiopatici, funzionano veri e propri sistemi computerizzati che raccolgono e forniscono informazioni vitali per il funzionamento, ad esempio, di *pacemaker* o *defibrillatori*: pertanto un'informazione erronea nei dati registrati nei *chips* e concernenti le cure, e comunque la propria storia clinica, potrebbe avere conseguenze serie sulla vita dei pazienti[7]. Non si deve trascurare poi il rilievo relativo al fatto che potrebbe verificarsi una diffusione incontrollata di dati sensibili, in considerazione del fatto che lo sviluppo delle tecnologie consente alle apparecchiature lo scambio di dati e informazioni con l'esterno, oggetto di possibile intercettazione nel circuito della Rete, con conseguenze potenzialmente irreparabili.

6 Cfr. il mio testo, *Internet Information e diritto penale,* Milano, 2010, p. 693 e segg.

7 Cfr., da ultimo, l'articolo di A. RUSTICHELLI, *Quando l'hacker attacca il pace-maker,* in *Affari e Finanza,* 7 giugno 2010.
Per quanto riguarda lo sviluppo della telemedicina ed il ricorso al *cloud computing*, vedi l'articolo di V. MACCARI dal titolo *"Hi-tech in ospedale. La cartella clinica sale sulla 'nuvola'"*,in La Repubblica, Affari e Finanza ,del 16/4/2012.

Ciò premesso deve dirsi che anche in Italia si sta verificando una tendenza all'introduzione dei R.F.I.D., definiti da un giornale specializzato (Il Corriere delle Comunicazioni, n. 19 del 9.11.2009) come *"oggetti prêt-à-porter"*.[8] Lo stesso legislatore italiano, nell'intento di proteggere alcuni prodotti nazionali, ha introdotto, senza tener alcun conto, tra l'altro. della sopracitata comunicazione della Commissione U.E., un sistema di etichette intelligenti. Il Parlamento ha infatti approvato la legge n. 55 dell'8 aprile 2010, recante il titolo *Disposizioni concernenti la commercializzazione dei prodotti tessili, delle pelletterie e calzaturieri,* allo scopo di permettere l'etichettatura dei prodotti *made in Italy*…[9].

La Commissione UE ha, inoltre, avviato una consultazione sulle normative necessarie per regolare la innovazione in questione in relazione alla connessione globale, tenendo conto degli effetti della evoluzione tecnologica sulla privacy, la sicurezza, l'etica e la

8 Rilevo, per inciso, che una recentissima applicazione dell'IdO è stata attuata in occasione dell'esposizione a Torino della Sindone, ad opera di una società multinazionale, la *Concet Reply*, che ha messo a punto una infrastruttura in grado di rilevare, attraverso particolari sensori e telecamere termiche, il succedersi dei pellegrini, di valutarne il flusso e la direzione e, in caso di necessità, di intervenire tempestivamente per mettere in atto le procedure di controllo necessarie. In proposito cfr. l'articolo di C. LA VIA, *L'Internet degli oggetti a servizio della Sindone,* 7 maggio 2008, in www.wired.it/news/archivio/2010.

9 L'articolo 2 della legge, al primo comma, si occupa delle norme di attuazione, stabilendo che "… 1. *Con decreto del Ministro dello sviluppo economico, di concerto con il Ministro dell'economia e delle finanze e con il Ministro per le politiche europee, da emanare entro quattro mesi dalla data di entrata in vigore della presente legge, previa notifica ai sensi dell'articolo 8, paragrafo 1, della direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, sono stabilite le caratteristiche del sistema di etichettatura obbligatoria e di impiego dell'indicazione "Made in Italia", di cui all'articolo 1, nonché le modalità per l'esecuzione dei relativi controlli, anche attraverso il sistema delle camere di commercio, industria, artigianato e agricoltura.* 2. *Il Ministero della salute, di concerto con il Ministero dello sviluppo economico e previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, adotta, entro tre mesi dalla data di entrata in vigore della presente legge, un regolamento recante disposizioni volte a garantire elevati livelli di qualità dei prodotti e dei tessuti in commercio, anche al fine di tutelare la salute umana e l'ambiente, con cui provvede, in particolare: omissis… …d) a stabilire l'obbligo della rintracciabilità dei prodotti tessili e degli accessori destinati al consumo in tutte le fasi della produzione, della trasformazione e della distribuzione".*

responsabilità. Ed ha anche pubblicato un questionario onde raccogliere tutte le possibili informazioni ed opinioni in ordine allo sviluppo **dell'IdO.**

Il Parlamento Europeo, in relazione alla Comunicazione della Commissione del 18 giugno 2009, ha emesso il 16 giugno 2010 una importante Risoluzione (2011/C 236 sull'Internet degli oggetti). Nei "*considerando*", tra l'altro, il Parlamento ha affermato che la tecnologia RFID può contribuire ad aumentare l'efficienza energetica e a ridurre le emissioni di gas a effetto serra, nonché a consentire il calcolo del carbonio a livello di prodotto. Il Parlamento ha inoltre richiamato l'attenzione dei Governi su punti importanti del fenomeno per quanto riguardava la protezione dei dati personali, affermando, tra l'altro, che per promuovere la tecnologia era indispensabile stabilire norme giuridiche che rafforzavano il rispetto dei valori fondamentali nonché della protezione dei dati personali e della vita privata. Il c.d.

Al riguardo è da osservare che una quasi incredibile negligenza del legislatore italiano in tema di allineamento alla normativa CEE ha dato luogo ad uno spiacevole incidente diplomatico in relazione all'iter della legge 55 del 2010 ed ai rilievi della Direzione Generale Impresa e Industria della UE (Nota n. 518763 del 28 luglio 2010). La Direzione in oggetto ha posto in luce un serio inadempimento dello Stato italiano alle disposizioni del Trattato e della Direttiva 98/34 CEE. In base a tali disposizioni gli Stati membri devono comunicare alla Commissione la bozza di regolamenti tecnici prima della loro adozione e comunque in uno stadio nel quale sia possibile adottare modifiche sostanziali. Lo Stato italiano, non si sa se per ignoranza o per negligenza degli addetti ai lavori, non ha ottemperato alle disposizioni sopracitate giacché la legge in questione, approvata definitivamente il 17 marzo 2010, è stata notificata alla Commissione soltanto qualche giorno prima (il 7 marzo, per la precisione). In relazione a tale legge è stata sollevata anche la questione relativa alla compatibilità della stessa con le disposizioni del Trattato sulla libera circolazione delle merci, in particolare per quanto concerneva etichettatura e l'indicazione di origine obbligatoria. I rilievi della Commissione hanno costretto il Governo a congelare di fatto (vedi in argomento la Direttiva del Presidente del Consiglio dei Ministri del 30 settembre 2010 e la nota dell'Agenzia delle Dogane del 22 settembre 2010, cui *adde* la nota di commento alla legge 55/2010 di A. Madeo, in questa rivista, n. 1/2011, pag. 19 e segg.) l'entrata in vigore della legge in questione, non emettendo i relativi decreti attuativi ,nonostante i disperati tentativi di uno dei presentatori delle leggi e dei suoi colleghi di partito della Lega Nord concretantisi in varie mozioni parlamentari). Nel frattempo il Parlamento Europeo ha approvato a larga maggioranza il 23/10/2010 il testo del Regolamento relativo alla indicazione del paese di origine di taluni prodotti qualora importati da Paesi terzi. Tale normativa non è in linea con quella italiana giacché quest'ultima prevede la etichettatura nei prodotti del tessile, delle pelletterie e delle calzature anche per le merci provenienti dai Paesi dell'Unione.

silenzio dei chips è stato preso in considerazione dal Parlamento in detta Risoluzione, citando l'opportunità della disattivazione automatica delle etichette presso il punto vendita, salvo espressa decisione contraria del consumatore, esortando i produttori a garantire il diritto al detto *silenzio* ,realizzando quindi etichette RFDI che possano essere rimosse o disattivate con facilità dal consumatore dopo l'acquisto ed esortando, infine, gli operatori dell'applicazione dei *tags* RFDI, ad adottare tutte le misure opportune per assicurare che i dati non siano collegati a persone fisiche identificate o identificabili.

2) IL CLOUD COMPUTING .CENNI SUI PROBLEMI TECNICI,ORGANIZZATIVI E LEGALI CONNESSI AL SUO USO

Passo ora ad accennare all'ultimo "grido" in fatto di applicazioni informatiche: mi riferisco al c.d. *cloud computing*.

Non si tratta di una nuova tecnologia: si tratta di una nuova metodologia dell'infrastruttura IT tramite la banda larga, concretandosi in una automazione dei servizi di gestione. Esistono indubbiamente dei benefici del *cloud computing* in quanto esso consente all'utente di ridurre notevolmente i costi associati alle forniture dei servizi: infatti appaiono sempre più numerose le aziende sedotte dalle offerte della società che forniscono i servizi di *cloud computing*, servizi che vengono ovviamente presentati dai fornitori come estremamente vantaggiosi dal punto di vista economico.

Sono tre le applicazioni principali del cloud computing, e cioè:

S a a s *(Software come servizio)*

Tale applicazione raggruppa la fetta più ampia del mercato relativo: essa può essere di qualunque tipo ,dalla gestione delle *e-mail* alle complesse applicazioni (tipo *google doc*) sino ad una serie di prodotti per la collaborazione *on line* (tipo *Rotus Live*).

P a a s *(Piattaforma come servizio)*

Essa fornisce al consumatore un ambiente di *runtime* per le sue applicazioni; permette eventualmente un parziale controllo nell'ambito in cui le applicazioni vengono eseguite.

La piattaforma in questione è quindi tipicamente un *framework* applicativo.

I a a s *(Infrastrutture come servizi)*

Tale applicazione fornisce quello che può definirsi come la fornitura di risorse computerizzate, di connettività, ecc. Il consumatore-utente ha il diretto controllo sul sistema operativo, sullo *storage*, etc. e può effettuare il *deployment*. In questo tipo di servizio gli utenti pagano in funzione dell'utilizzo che faranno delle risorse: viene quindi anche chiamato *utility computing*[10].

L'aspetto caratteristico del *cloud computing* è che il fenomeno è connesso alla possibilità, sfruttando la velocità della banda larga, di utilizzare *hardware* e *software* ubicati, dal punto di vista della localizzazione geografica, in una qualunque parte del mondo.

10 Secondo l'uso si distinguono tre tipi di *cloud* e cioè il *public cloud*, creato da un venditore ed offerto al pubblico; il *private cloud* che è ospitato dalla stessa organizzazione che utilizza il servizio; l'*hybrid cloud* che si riferisce ai casi di organizzazioni che hanno messo in opera i *private cloud services* in combinazione con gli *external public cloud services*. Questo termine si riferisce anche ai servizi offerti ed usati esclusivamente da uno specifico gruppo invitato di utenti privati ed è chiamato anche *community cloud* (vedi al riguardo il *paper* dal titolo *Cloud Compunting – deep dive*, del gennaio 2011).

Tuttavia vi è il rovescio della medaglia e cioè, come diremo più innanzi, esistono rischi e pericoli nell'uso e nella gestione del *cloud computing*. Varie organizzazioni hanno esaminato il problema, tra cui la citata ENISA, l'Ente Europeo che dovrebbe occuparsi della sicurezza informatica, che ha redatto un apposito studio dal titolo *Cloud computing – benefit, risk and recommendations for IT security.* L'ENISA, in particolare, ha elencato e descritto 35 rischi dei quali ben 23 specifici al *cloud computing*.

Più particolarmente, secondo lo studio, i rischi organizzativi sarebbero 7, quelli tecnici 11, quelli legali 15. Le vulnerabilità del sistema sarebbero in totale ben 38! In effetti, nonostante le grandi campagne pubblicitarie condotte dalle imprese che commercializzano il sistema (vedi infra), non sembra che, almeno per il momento, l'ambiente interessato si sia dimostrato molto recettivo.

Va detto a questo proposito che la società *Forrestar Researce inc*., una società di ricerca indipendente, ha effettuato una indagine *ad hoc*, interpellando, nel 2010, oltre duemila IT *executive* e *decision's makers* in tema di IT, in Canada, Francia, Germania, UK e USA. I soggetti interpellati hanno mostrato uno scarso interesse al sistema *pay as pay hosting* dei servizi virtuali e degli altri servizi offerti dal *Cloud Computing*. Soltanto il 3% ha dichiarato, infatti, di usare il sistema: la percentuale è rimasta fissa rispetto all'anno precedente.

3) CONVEGNI SUL COULD COMPUTING ED OPINIONI NA CONFRONTO,. IL MARKETING ALL'ASSALTO DELLE PMI E DELLA P.A.

L'argomento del *cloud computing* e dei suoi vantati pregi dal punto di vista della sua economicità ed efficienza, è stato oggetto di alcuni convegni svoltisi recentemente in Italia e, *pour cause*, a Roma soprattutto, nel corso dei quali è sembrato, però, che i pericoli ed i rischi di vario genere, indubbiamente legati all'uso dell'applicazione in questione, siano stati trascurati dai relatori o, al massimo, siano stati oggetto di qualche frasetta di circostanza,(tanto per salvare la faccia) in ordine alla sicurezza o alla *privacy.*

Ad esempio, il Convegno, avente come titolo: **Pubblica amministrazione che si trasforma: cloud computing, interoperabilità – proposte al governo**, indetto da Astrid-Think il 20 marzo 2012 in Roma, si è limitato, in sostanza, ad illustrare i benefici possibili in tema di efficienza dei servizi per la PA, totalmente dimenticando i possibili, e ormai noti, rischi in tema di sicurezza e *privacy* e, soprattutto, omettendo qualsiasi accenno ai rischi ambientali (vedi *infra*) collegati allo sviluppo delle *farms informatiche* per quanto riguardava clima e salute pubblica…

Il tema del *cloud computing* è tornato alla ribalta lo scorso anno nell'ambito del consueto annuale FORUM (2011) della PA, nota rassegna pubblicitaria del settore indetta da una società che gestisce convegni e incontri tra pubbliche amministrazioni ed imprese. Una sezione del FORUM dello scorso anno è stata infatti dedicata al tema in oggetto; il titolo dell'incontro, (involontariamente ironico, date le circostanze…), è stato "LA PA SULLA NUVOLA"…(vedi gli atti nei Quaderni del Forum PA, del febbraio 2012)... Inutile dire che il tema della sostenibilità ambientale dello sviluppo del *cloud computing*, di

estremo interesse pubblico, è stato accuratamente evitato.. di tutto si è parlato tranne che dell'argomento sopra citato…. In tale manifestazione si è verificato il consueto "abbraccio" tra grandi fornitori e aspiranti fornitori della PA da una parte, il DigitPA, il Garante della Protezione dei dati personali e altri rappresentanti delle istituzioni, dall'altra.. In questo ambito si è tenuta anche la *"Prima Conferenza del cloud computing nella PA"*, dando gli organizzatori evidentemente per scontato, con singolare preveggenza, che *"... la storia avrebbe avuta una lieta fine per il Paese..."* con ciò sottintendendo, evidentemente, che i *"decision's makers"* pubblici avrebbero alla fine convalidato la scelta (fortemente ed ovviamente auspicata da tutti gli intervenuti) di lanciare *"..la PA sulla nuvola* (***sic***)"… non si sa se dotata o meno di efficienti paracadute …

Scorrendo gli atti del sopracitato Convegno si intuisce che il dialogo si è svolto in forma, come dire?, di minuetto settecentesco tra i venditori ed i rappresentanti delle istituzioni presenti, … Il sopracitato Garante, ingaggiato nel coro e trascinato dall'entusiasmo, si è perfino spinto a pronunciare frasi storiche del tipo *"...non ci sono alternative... sarebbe da irresponsabili opporre delle resistenze...",* frasi opportunamente utilizzate come slogan dagli organizzatori del convegno, (vedi al riguardo l'introduzione di R. Masiero). Per dovere di cronaca non si può trascurare di citare in argomento il "Benussi-pensiero",uno dei collaboratori del Ministro Profumo che ,in una intervista al Corriere delle Comunicazioni del 4 luglio, ha dichiarato solennemente "….Nuvola e servizi as a service sono chiavi per

favorire un cambiamento nell'organizzazione del lavoro nella pubblica amministrazione…."!!

Sul tema del *cloud computing* gli organizzatori del FORUM PA hanno deciso di continuare a "battere il chiodo" ed infatti nella successiva manifestazione (16/19 maggio 2012) hanno insistito sull'argomento del *"Government-cloud…",* inserendolo come uno degli argomenti centrali dalla manifestazione stessa. Con ciò rivelando in qualche modo, ancora una volta, gli intenti sopratutto di *marketing* dell'organizzazione… ed, in particolare, il proposito di coinvolgere decisamente le istituzioni nel mercato dei servizi *cloud computing*[11].

A proposito ora delle nuove applicazioni e della loro introduzione nei settori pubblici, va detto che il complesso sistema informatico delle

11 Nell'ambito della campagna mediatica- promozionale del *marketing* sul *cloud computing* spicca il Convegno dell'ottobre del 2011 organizzato a Roma dal periodico Corriere delle Comunicazioni, ma in realtà sponsorizzato dalle organizzazioni fortemente interessate quali Telecom Italia, HP, Emc e Trend Micro ,convegno che ha reclutato, accanto ai rappresentanti degli *sponsors*, anche rappresentanti delle istituzioni (Senato, DigitPa, Ministero PA; vedi, al riguardo, l'articolo dal titolo … che è tutto un programma… *Cloud, imperativo per la P.A*. pubblicato nel detto periodico. Dall'intervento del Presidente della DigitPA si è appresa comunque una notizia interessante, e che forse doveva rimanere segreta… e cioè che *"...DigitPA ha battezzato (**sic**) un gruppo di lavoro che, con il supporto dell'Enisa (l'Agenzia per la sicurezza delle reti e dell'informazione)* (organizzazione, questa, peraltro snobbata dalla quasi totalità degli Stati europei e, opportunamente, parcheggiata a Creta… n.d.r.) *ha il compito di varare le linee guida sull'adozione del cloud nella PA. Al tavolo partecipano circa (**sic**) 100 esperti provenienti dal mondo dell'impresa, dell'Università e della Pubblica Amministrazione…"* Si vede che questa supercommissione stava lavorando nel massimo segreto … giacché della sua esistenza, almeno sino ad oggi, non vi è traccia nel sito della DigitPA, sempre ridondante di notizie circa le attività che si afferma svolte dall'ente a livello nazionale ed internazionale…Una" lucina" tuttavia è recentissimamente ,apparsa nel buio,,, In un *paper* presentato dalla DigitPA al Forum Pa il 14 maggio 2012 dal titolo "*Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione…"* nella Premessa si dice che era stato costituito (ma non si dice in quale data) un gruppo di lavoro in ordine al *cloud,* comprendente, si afferma "*..esperti, amministrazioni, aziende ed altri organismi attivi nel settore…*", gruppo che avrebbe,s i dice"….. *prodotto un materiale*", (**sic**), del quale, però, si ignora, la natura e la consistenza. Segue una formula criptica che vale la pena di riportare, testualmente,"… *Il presente testo di raccomandazioni e proposte è il risultato di una elaborazione autonoma di DigitPA condotta sul materiale prodotto dal gruppo di lavoro...*" Ma allora il decantato gruppo si sarebbe limitato a raccogliere del materiale? Mistero! Ritornando all'argomento principale, dalla fonte congressuale sopracitata, apprendiamo che la DigitPA non solo non dorme in ordine al *cloud* ma anzi addirittura … *"ha investito 5 milioni di euro per il progetto M@eCloud, lanciato in collaborazione* con *il Ministero degli Affari Esteri…"* progetto che *"...mira a creare una "nuvola" si condivisione delle risorse a disposizione delle 325 sedi internazionali della Farnesina per aumentare l'efficacia dei servizi…" ...* Al riguardo, intese anche le critiche degli esperti al progetto, non resta che sperare nell'opera del Commissionario Governativo alla *spending rewiew*, . Enrico Bondi. il cui compito è quello di razionalizzare la spesa pubblica mediante i tagli. …

FF.SS, una infrastruttura vitale del paese, sembrerebbe sul punto di *"...passare da un preesistente sistema di outsourcing al cloud computing..."* in quanto, secondo quanto affermato da un infervorato dirigente dei sistemi informatici della FF.SS., Musumeci, in una intervista resa al periodico *"Corriere delle Comunicazioni,"* e pubblicata nel n. 14 s del 19/9/2011, si tratterebbe di *"...una scelta irreversibile..."* Le indubbie criticità del nuovo sistema, individuate dall'intervistato come *"...sicurezza e salvaguardia dei dati personali...",* vengono liquidate come *"...uno dei due punti di attenzione..."* ma né vengono citati i costi organizzativi ed economici della trasformazione del sistema né l'intervistato chiarisce, quale era l'altro "punto di attenzione"…[12]

Per dovere di cronaca occorre tener presente in argomento che la DigitPA, ente molto discusso (pur se scaturito dal cervello dell'allora noto "Giove" di turno…) che ha preso il posto del CNIPA, (organizzazione questa alle dipendenze dall'ex Ministro Lucio Stanca distintasi, tra l'altro, negli anni precedenti per l'attenzione al problema della sicurezza dei sistemi informatici pubblici.. ma soppressa rapidamente appena costituita la penultima compagine ministeriale berlusconiana,) ha divulgato una notizia di *"vitale importanza"* e cioè

12 Anche la CONSIP sembra abboccare all'amo del *cloud computing,* almeno a giudicare da una intervista recentissima resa dal suo dirigente, D. Casalino, al periodico Corriere delle Comunicazioni del 23 aprile 2012, nella quale si afferma che… *"Per il MEF stiamo progettando l'architettura cloud di tutti i Ced, ossia di quelli in capo al Dipartimento del tesoro, alla Ragioneria Generale dello Stato ed al Dipartimento Affari Generali".* Il Dirigente sopracitato ha affermato poi che l'operazione (che in prospettiva dovrebbe riguardare tutti i 1033 Ced dell'Amministrazione centrale) genererebbe un *"...immediato risparmio di costi... ed anche di consumi energetici...*" A parte la "balla" sul risparmio energetico, il Dirigente citato non spende neppure una parola sui costi e sui problemi organizzativi dell'operazione e nulla dice sui problemi connessi della sicurezza e della *privacy* …

che questa organizzazione sta lavorando, nientemeno, con il Governo della Corea del Sud, per digitalizzare lo scambio di documenti fra tutti i soggetti coinvolti nel traffico navale Italia-Corea e ritorno e sviluppare una prima *app on the cloud* gratuita!! C'è poco da scherzare, sul piatto, ci informa il Corriere delle Comunicazioni del 18 novembre 2011, ci sono ben 10 milioni di euro!![13]

4) RISCHI SPECIFICI TECNICI,ORGANIZZATIVI E LEGALI CONNESSI ALL'USO DEL CLOUD COMPUTING

Alcuni studiosi(vedi L.Bolognini ed altri, nel capitolo intitolato *Cloud computing e protezione dei dati personali:privacy e web globale rischi e risorse,*nel volume collettaneo, *Next Privacy*,,Milano,2010) vedono nello sviluppo dei grandi *data center* un rischio per la concorrenza ed affermano che lo sviluppo di un *data center* abbastanza capace per il mercato del *cloud computing*, richiede ingenti somme di denaro ciò costituirebbe "… *una barriera*

13 Peraltro, gli scarsi risultati della informatizzazione della P.A., e quindi dell'opera del DigitPA, sembrano emergere anche dalle incisive dichiarazioni rese da un alto funzionario della struttura ,il Direttore Generale Giorgio DE RITA, in un contributo realizzato per Nomisma, Iconsulting e la stessa DigitPA sulla *business intelligence* (è detto proprio così, non stiamo facendo dell'umorismo nero) nel settore pubblico. De Rita ha dichiarato testualmente *"…Servivano forse più coraggio, forse più incoscienza, forse meno soldi disponibili, forse maggior controllo della opinione pubblica. Sta di fatto che è stata una fra le tante occasioni perse…"* (vedi l'articolo di S. CARLI dal titolo *Lo Stato digitale non è "intelligente"*, in Affari e Finanza del 7 novembre 2011). L'articolista così commenta, in modo lapidario, tale dichiarazione *"…E che si parli di business intelligence e non solo più di digitalizzazione è significativo: di digitale nella PA italiana ce n'è molto, di intelligenza poca…"*.
Va in proposito rilevato che alquanto deludenti sono state le iniziative di approccio tecnico- organizzativo e culturale ai problemi della introduzione del *cloud computing* nelle pubbliche amministrazioni… I seminari organizzati sull'argomento dalla DigitPa (*Giornate di studio su governement e cloud computing,* dell'8 ottobre 2010, e *Seminario su nuove tecnologie, biometria cloud computing e sicurezza,* del 25 febbraio 2011) si sono risolti, il primo -in gran parte- in una specie di "vetrina" degli aspiranti fornitori… ed il secondo in una specie di rassegna su fumose iniziative di virtualizzazione di un paio di *data center* di amministrazioni pubbliche.

all'ingresso di nuove aziende nel mercato cloud con conseguenti disastrose per la concorrenza e la data protection… più è spinta la concorrenza minore sarà il periodo di concentrazione di dati nei servet di pochi colossi informatici…"[14].

Detto per inciso, i " venditori ", del *cloud computing* non sembrano preoccuparsi dei problemi giuridici relativi dell'applicazione in questione…[15] Il pericolo della incertezza giuridica relativa ala regolamentazione del *cloud computing* è stato, invece, avvertito esplicitamente, con molta sensibilità, dal Parlamento Europeo nella Risoluzione del 15 giugno 2010 sull'Internet degli oggetti (vedi infra)

14 Il *paper* dal titolo *Is the Cloud killing your commerce*? pubblicato in *Compuware Gomez – Performance in the Cloud*, Survey Report 2011, esamina *"...the risk that online retailers face by ceding control of application to CSPs (Cloud Service Providers)...* ed afferma, tra l'altro, che *"...Among the top retailers, 40 percent use Amazon Web Service ... and across the top 50 retailers there are 107 separate out sourced application in use. Yet, organizations in North America are losing on average almost $ 1 milion per years because of the poor performance of their cloud-based applications. In Europe the figure is more than $ 0,75…".*
Circa il ricorso da parte degli SMB alla tecnica del *cloud* vedi l'articolo dal titolo *"SMBs Launch into Cloud Computing and Virtualization in* www.hp.com/go/vmware ed *il paper* reclamistico di IBM dal titolo *"IBM Smart Cloud-Enterprise Infrastructure as a service"* recante il solito slogan-specchietto per le allodole *"... Increase business agility and cost efficiency with cloud computing for enterprises and their partners."*

15 In realtà le "Old Fox" si stanno organizzando in vista dell'allargamento della fornitura *Cloud* alle "gallinelle", sinora alquanto riluttanti, delle PMI (vedi al riguardo l'articolo di L. Ferro dal titolo *Alleanza Telecom-Microsoft. Avanti tutta sul cloud per PMI,* nel Corriere delle Comunicazioni del 23 aprile 2012).
In ordine alle notizie più recenti in ordine alle campagne pubblicitarie delle grandi imprese, vedi gli articoli di G. Gerino dal titolo *Dal cloud computing ai "big data": Oracle propone soluzioni per tutti"* e l'articolo dal titolo *"Adobe CS6 disponibile sulla "nuvola",* entrambi in Affari e Finanza del 30 aprile 2012. cui *adde* l'articolo di L.Ferro, dal titolo *Microsoft lancia il"cloud all-in-one,* in Corriere delle Comunicazioni del 17 maggio 2012.
Tuttavia, secondo alcun esperti (vedi l'articolo dal titolo *SMB Cloud Is A Hacker*? *Paradise* (http://Cloudcomputing.sys_con.com/mode), la diffusione del *cloud computing* presso gli SMB (*Small and medium-sized business)* rappresenterebbe una vera pacchia per gli *hackers, f*avoriti dalla ignoranza degli utenti,dalla 'apatia dei providers e dall'alto costo della sicurezza La circostanza è avvalorata da un recentissimo paper della Symantec dasl titolo Symantec Intelligence Report" pubblicato nel giugno scorso ,secondo cui ,nell'utimo semestre il 36% degli attacchi hacker è stato diretto nei confronti di aziende con 250 dipendenti o meno (vedi l'articolo dal titolo "Malware:sotto sttacco le piccole aziende" pubblicato nel Corriere delle Comunicazioni del 23 luglio).. Occorre correggere pertanto l'errata opinione dei gestori di *small business* i quali *"...often think that hackers are only interested in attacking large compagnie and government agencies" …* giacché, in realtà"... *most hacking schemes benefit from the availability of large numbers of unprotected systems..."*in argomento va ricordato che il Garante per la protezione dei dati personali ha diffuso un utile libretto ,contenente una miniguida per le imprese e per la PA dal titolo "Cloud Computing.Proteggere i dasti per non cadere dalle nuvole" nel quale,tra l'altro,richiama l'attenzione delle imprese e della stessa PA i ordine ai rischi connessi all'adozione deln cloud computing ,anche in relazione alla protezione dei dati…

al punto 48 dei "*considerando*". Anche John Vassallo, responsabile degli affari regolamentari di Microsoft nell'ambito U.E., in una intervista al periodico Corriere delle Comunicazioni del 2 aprile 2012, dopo aver riconosciuto che *"...Paura, sfiducia, timori per la sicurezza sono gli ostacoli da superare per la diffusione industriale del cloud..."* ha dichiarato che… *"Nell'UE auspichiamo l'adozione di un quadro regolamentare chiaro e meno frammentato su privacy e data protection..."*. Dal canto suo l'organizzazione denominata *Electron Privacy Information Center* ha rivolto un appello al Congresso USA, affermando che occorreva bloccare i richiami, immotivati e pericolosi, al *cloud computing* e le sue promesse: le *appliance* di *Google* avrebbero dovuto essere tenute sotto chiave sino a quando non l'organizzazione non fosse stata in grado di offrire garanzie sufficienti agli utenti. In pratica l'organizzazione sopra indicata ha chiesto alla FTC *(Federal Tecnological Commission)* di impedire a *Google* di continuare a somministrare le proprie *appliance* fintanto che la società non fosse stata in grado di dimostrare che le sue pratiche erano adeguate, sicure e rispettose della *privacy.*

Per il momento la FTC ha deciso di chiamare a raccolta le aziende attive nel *cloud computing*, onde interpellarle al fine di stabilire se

fosse più o meno opportuno rendere le regolamentazioni più stringenti[16].

Di *cloud computing* si parla anche fuori degli Stati Uniti, ad es. in seno all'OCSE. Nell'ottobre scorso (2009), poi, l'Unione Europea ha aperto un tavolo di consultazione per l'eventuale revisione della Direttiva sulla protezione dei dati personali che dovrebbe essere ammodernata per prendere in considerazione tra l'altro, i rischi del *cloud computing*[17].

Giudizi severi, peraltro, circa l'enfasi adoperata da alcuni sostenitori ad oltranza della novità ed importanza assoluta del *cloud computing* sono stati dati da esperti come *Larry Ellison*, il fondatore di *Oracle*, secondo cui… *"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. The computer industry is*

16 Un documento molto interessante la cui lettura, sia detto tra parentesi, andrebbe sommessamente consigliato ai nostri *decision's makers* allorché decidono di occuparsi dell' adozione nel settore pubblico del *cloud computing* è il *paper* dal titolo *Federal cloud computing strategy*, redatto da V.Kundra,U.S. Chief Information Officer, e pubblicato l'8 febbraio 2011. Va osservato, però, che l'interessante studio sembra dimenticare completamente l'impatto sull'ambiente derivante dalla introduzione del *cloud*…ed infatti un autorevole commentatore, il CIO B. Golden, ha osservato, in una nota dal titolo " *Federal Government's Plan. A $ 20 billion shift"*, che il *paper* in questione "*… As is the nature of many government publications its flat prose downplay the critical implications of the content…."* (http://www.cio.com/article/print/671013.

17 La divisione di *Emerson "Emerson Network Power*" leader internazionale nella ottimizzazione della disponibilità, della capacità e dell'efficienza delle'infrastrutture critiche, ha tentato di fare un po' di chiarezza per dissipare la "nuvola pubblicitaria" che avvolge il *cloud computing,* picconando i più noti e falsi miti della interessata manovra propagandistica commerciale … tipo *"tutti stanno passando al cloud",.. "con il passaggio al cloud non ci si deve più preoccupare dei tempi di fermo".. "la nuvola riduce sempre i costi ed il carico di lavoro" ...* (vedi l'articolo relativo dal titolo *"Realtà e fantasia in tema di cloud computing"*, in *http://www.thedailybit.net/index.php?method=news&action=zoom&id=11560&f* .

the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish[18]*. It's insane. When is this idiocy going to stop?"*

A sua volta sull'argomento va giù pesante *Richard Stallman*, (fondatore di *Free Software Foundation*), affermando testualmente… *"One reason you should not use Web applications to do your computing is that you lose control. It's just as bad as using a proprietary program. Do your own computing on your own computer with your copy of a freedom-respecting program. If you use a proprietary program or somebody else's Web server, you're defenceless. You're putty in the hands of whoever developed that software"*[19].

18 *Gibberish* è un termine di slang che indica, secondo Wikipedia, un borbottio, senza senso. Si tratta di un termine generico che in inglese indica il parlare usando suoni simili a parole, ma che non hanno alcun significato reale. Questo significato è stato esteso anche ad un testo senza senso o incomprensibile (es. supercazzola). Il tema comune nelle istruzioni senza senso è una mancanza di senso letterale, che può essere descritto come una presenza di sciocchezze e *nonsense.*

19 In definitiva STALLMAN, fondatore della *Free Software Fondation*, ha definito il *cloud* come una mossa tipicamente pubblicitaria che metterebbe i dati degli utenti su *server* remoti, in balia dei fornitori dei *server* stessi. In una intervista al *Guardian* ha poi dichiarato testualmente che *"… il cloud computing è roba di stupidi e utilizzare applicazioni web come Gmail di Google è anche peggio della stupidità stessa…"* e ha aggiunto: *"… Un motivo per cui non dovresti usare applicazioni web per il tuo lavoro è che ne perdi il controllo", "E lo stesso vale per i programma proprietari. Se usi programma proprietario o il web server di qualcun altro, sei nelle mani di chiunque abbia sviluppato quel software"*. Stallman ha anche liquidato lo *hype* del *cloud computing* come *"..Una completa idiozia. Al peggio una campagna di marketing in un'industria legata alle mode anche più di quella dell'abbigliamento femminile"*. Vedi anche, in argomento, l'intervento reso da Stallman in occasione di una visita all'Università delle Calabrie, riportato nell'articolo dal titolo *Richard Stallman: l'ultimo degli hacker,* in www.linusks-magazine.it nel quale ha sostenuto, senza mezzi termini che *"… il cloud computing limita, e non poco, le nostre libertà soprattutto in tema di sicurezza e di privacy"*. Infine vedi l'articolo di B. WAFFING, *Richard Stallman: cloud computing a trap,* in www.linusks-magazine.com, 1° ottobre 2008,cui *add*e il frizzante articolo dal titolo *Ethics and the Cloud* di K.W. MILLER e J. VOAS, esperti del NIST (National Institute of Standards

5) IL CLOUDCOMPUTING ED I SUOI RISCHI PER L'AMBIENTE

La nota organizzazione *Greenpeace* ha esaminato i rischi ambientali del *cloud computing* in un suo recente rapporto dal titolo *"MAKE IT GREEN"* ,sottotitolo*, Cloud Computing and its Contribution to Climat Change),* frase che costituisce anche il titolo della relativa campagna di informazione. Il rapporto esamina il grave problema delle emissioni di CO_2 prodotte dai *"servers"* che si occupano del funzionamento della "nuvola" e che sarebbero in gran parte alimentati a carbone e quindi altamente inquinanti. Inoltre essi consumerebbero miliardi di KW di energia per il loro funzionamento, soprattutto per le enormi necessità di raffreddamento dei macchinari del *"data center"* occorrenti per la costruzione delle "nuvole", tanto che le *"farms"* devono essere costruite vicino a fiumi o laghi o addirittura su piattaforme marine. Le preoccupazioni per la futura eco sostenibilità delle applicazioni *cloud è* chiaramente espressa da *Greenpeace* allorché nel rapporto afferma che… *"2010 has been touted by many in the ICT sector as the 'Year of the Cloud'. While this likely a prediction that will be*

---

and Technology), pubblicato da IEEE *Computer Society* in IT PRO-2010. Vedi, in argomento anche l'articolo di J. BRODKIN dal titolo *"FAQ: Cloud Computing, demystified,* in Network World, http://www.networkworld.com/supp/2009ndc3/051809-cloud-faq-html.

repeated in subsequent years. The arrival of the iPad and growth in netbooks and other tablet computers, the launch of Microsoft'Azure cloud services for business and the launch of the Google phone and the proliferation of mobile cloud application are compelling signs of a movement toward clod-based computing within the business sector and public consciousness in a way never seen before…". Il rapporto attacca principalmente "Facebook", il notissimo *social notework*, che ha costruito un gigantesco *"data center"* nell'Oregon utilizzando, secondo *Greenpeace,* come carburante il carbone, materiale altamente inquinante. Ma anche altre aziende tra cui *Apple, Microsoft, Yahoo* e *Google* utilizzano il prodotto di cui sopra… La gigantesca espansione delle *"farms"* è documentata dalla costruzione dello *Yahoo Data Center* (Lockport, N.Y.) di *Buffalo* costato oltre 150 milioni di dollari. e dalla *"farm"* di *Apple Computer* (North Carolina, U.S.) costruita presso identico centro *Google* e costata circa un miliardo di dollari. *Google*, inoltre, ha costruito nei pressi di *Dallas* nel 2006 due *"farms"* sul bordo del fiume Columbia per disporre di acqua per il raffreddamento…[20].

Nel 2010 *Google* avrebbe rilasciato nell'aria 1,46 milioni di tonnellate di anidride carbonica, l'equivalente della combustione

20 Secondo il periodico Computer Idea (vedi l'articolo dal titolo *Google quanto consuma?* del 18.10.2011), il V.Presidente della *company* avrebbe ammesso che solo nel 2010 *Google* avrebbe consumato qualcosa come 2,3 milioni di KW ovvero 41 volte l'elettricità consumata dall'intero *Empire State Building* nel corso di un anno...

respiratoria di 70mila persone… A proposito poi della *"privacy"* degli utenti, va detto che *Google* ha aperto il nuovo servizio *"cloud",* denominato *Google Drive*, precisando, nella licenza d'uso, che si riservava il diritto di "usare, ospitare, immagazzinare, riprodurre, modificare o creare versioni derivate, pubblicare, mostrare pubblicamente, comunicare o distribuire" il contenuto caricato sui suoi servizi (così l'articolo dal titolo *Google Drive, sulla nuvola*, di C. Tamburrino, in hptt://punto-informatico.it,del 26.4.2012.

Sempre secondo *Greenpeace*, l'introduzione del *cloud computing* influenzerà il settore dell'ICT, determinando per il 2020 un consumo totale di quasi **duemila miliardi di kilowattore di elettricità**, cioè il triplo del consumo attuale, e più del consumo elettrico di Francia, Germania, Canada e Brasile messi insieme!!! [21]

Un successivo rapporto dal titolo *"How dirty is your data?"* (sottotitolo *"A Look at the Energy Choices That Power Cloud Computing*), è stato presentato l'anno scorso (2011) a San Francisco sempre da *Greenpeace* in occasione della *Green Net Conference.* Si tratta di uno studio che effettua una accurate analisi di dieci grandi imprese, e cioè *Akamai, Amazon Web Service,*

Secondo qualche esperto (così R.M. Katz., *Tech Titans*, in Spectum Magazine, febbraio 2009 citato da D. GUINIER nell'articolo dal titolo *"L'informatique dématerialisée en nuage"* in Expertises, ottobre 2010) la concentrazione di un milione di servers in una *mega-farm* esigerebbe una potenza elettrica di un terzo di quella fornita da uno dei due reattori della centrale nucleare francese di *Fessenheim*… Si tenga presente, comunque, che *Google* già dispone, come afferma Guinier, di oltre due milioni di *server*s sparsi nel mondo e già Microsoft prevedeva di disporne entro il 2011 di più di un milione…

Apple; Facebook, Google, Hewlet-Packard-IBM, Microsoft e Yahoo. L'importante rapporto cerca di rispondere ad una fondamentale domanda e cioè *"... As cloud technology disrupt our lives in many positive ways, are the compagnie that are chancing everything failing to address their own growing environmental footprint?..."*

Il rapporto rivela, tra l'altro, una importante circostanza e cioè che esiste nell'ambito del settore specifico interessato una grande ipocrisia: infatti mentre *"...broady declare trasparency as major tenet of their business model..."* in realtà *"...are highly secretive about their own operation..."*. E pertanto il velo del segreto rende quasi impossibile misurare gli attuali benefici della tecnologia

---

21 Secondo il rapporto, regole come quella del PUE *(Power Usage Effectiveness)* e del DCE (*Data Center Infrastructure Efficiency),* si limitano ad accertare la efficienza delle infrastrutture dei *data centers* in relazione alla energia richiesta. Il rapporto afferma inoltre che… *"Government Institution like USEPA and industry association like Green Grid (which established PUE) have been largely complicit..."* nel mancato accertamento dell'effettivo tasso di *"dirty energy"* necessaria per i nuovi *data centers*. Per quanto riguarda i costi sanitari ed ambientali umani (malattie, morti, inquinamento idrico ed atmosferico, ecc.) imputabili all'uso del carbone ed alle emissioni del CO_2, il rapporto citato, a pagina 4, ne fa una sommaria ma altamente preoccupante analisi. A proposito della *Trasparency and Reporting* giustamente il rapporto sottolinea la circostanza che il rifiuto da parte delle società di rivelare il tipo di energia adoperata e le fonti di energie fornite per le loro piattaforme *"... we are left in the dark with renard to the net impact that cloud computing has on carbon, and thus our own use related emissions..."* Molte società giustificano la mancanza di trasparenza affermando che le relative informazioni costituiscono *"... a trade secret"* che potrebbe essere usato dai loro competitori… in realtà società come IBM, Cisco e Wipro, che hanno dimostrato maggiore trasparenza circa i dati rispetto ad altre società del settore interessato, non sembrano avere avuto nessun effetto commerciale negativo. In definitiva il rapporto, esaminando vari fattori, indica come maggiori produttori di *"coal intensity" Apple* (54%) *Facebook* (53,2%) *IBM* (51,6%) HP (49,4%) *Twitter* (42,5%) *Google* (34,7%) *Microsoft* (34,1%). I "virtuosi", si fa per dire, risulterebbero *Amazon* (28,5%) e *Yahoo* (18,3%). Vedi in argomento l'articolo dell'Espresso del 28 luglio 2011 dal titolo "*Quanto inquina Internet*?", di D. CORINTO..In tema di poteri delle amministrazioni USA di accesso ai dati delle imprese che esternalizzano i loro sistemi di infornmazioni,vedi l'articolo di Blin-Gabadou dal titolo *"Cloud Computing_Mythes et rèalitès du Patriot Act*",in *Expertises* del dicembre 2011..

cloud o rendersi conto se lo sviluppo delle apparecchiature IT si traduca in un aumento in tema di richiesta di elettricità e se questo, di riflesso, produca un aumento dell'uso della *"dirty energy"*. Sta di fatto che le società interessate rifiutano pervicacemente di rilevare la quantità di energia consumata, le emissioni di CO_2, la quantità di scorie nucleari prodotte come risultati del mantenimento della loro infrastruttura digitale. In definitiva, secondo il rapporto, si continuerebbe ad usare la "*dirty energy*" per la produzione, esattamente come nel XIX e XX secolo, e ciò nonostante i moniti degli scienziati i quali affermano che il carbone e le centrali nucleari sono largamente responsabili per il livello catastrofico dell'inquinamento mondiale!!! [22]

Greenpeace, pur in considerazione della riluttanza delle grandi imprese, a rivelare i dati, è riuscita comunque ad ottenere sufficienti elementi, servendosi di indici relativi agli investimenti per i *data centers* ed effettuando una analisi selezionata delle infrastrutture scelte delle maggiori imprese nel settore del *cloud computing*. Ed a proposito dei *data centers*, le cui dimensioni in

---

22 Secondo una dichiarazione dell'IEA resa nell'autunno del 2011 ... *"unless a decisive shift is made to clean Energy investment and away from high-carbon sources of Energy like coal, in the next five years (by 2017), the Earth will be locked into a disastrous cycle of unavoidable global warming*...Secondo recentissime notizie di stampa (vedi l'articolo di Hertsgaard dai titolo " *E'finita l'età del carbone "*,in La Repubblica del 6 giugno) in USA l'Agenzia EIA (Energy Information Administration) ,specializzata in analisi energetiche ,ha anche annunciato che solo il 36% del fabbisogno del Paese è coperto da fonti inquinanti come il carbon fossile,con un calo di venti punti rispetto all'anno precedente.L'EIA prevede,,inoltr.e,un calo ulteriore entro la fine del corrente anno.

genere non vengono rivelate, e spesso effettuate, come dice il rapporto, *"out of public eye"*, il rapporto medesimo rileva, per esempio, che in USA, paese che ospita circa il 40% dei *servers* mondiali relativi ai *data centers*, è stato stimato che il consumo di questi *servers* supera il 3% della disponibilità nazionale. Ad esempio, il nuovo *data center* della *Apple* nel North Carolina, costato oltre un miliardo di dollari, consumerebbe quanto 80.000 dimore statunitensi o 250.000 dimore della UE. Anche quest'anno (aprile 2012) *Greenpeace* ha presentato il suo rapporto dal titolo "*How Clean is Your Cloud*?" nel quale sottolinea che la scelta del tipo di energia dedicata alla espansione del fenomeno… "*are completely invisible to consumers*…" Nel rapporto si afferma, inoltre, che tre delle più grandi società che gestiscono i loro affari nel settore cloud, *Amazon, Apple Microsoft,* stanno rapidamente espandendo la loro attività nel settore… "*without adeguate renard to source of electricity, and rely heavily on dirty energy to power their clouds*…" Il rapporto richiama una importante dichiarazione dell'IEA *(International Energy Agency* (vedi nota 22) ed esamina le *locations* delle infrastrutture *cloud* in varie parti del mondo (Germania, Honk Kong, Irlanda, Olanda, Svezia) ed in vari Stati USA (Illinois, North Carolina e Virginia, Washington e Oregon) e la percentuale dei prodotti usati per la produzione di elettricità… in testa per l'uso del carbone è Hong Kong (54%) seguita dalla

Germania (44%). L'Olanda appare la più virtuosa (19,5%). In Usa, area di Chicago, si è al $$%, nella North Carolina al 61%, in Virginia al 45, nell'Oregon al 61%. Allo scopo di raggiungere due dichiarati input (*1) Extimated size of electricity demand of each facility in megawatts; 2) Amount of renewable electricity being used to power it,*) il rapporto ha tracciato una plausibile graduatoria *(CleanEnergy Index)* delle varie Companies (*Akamai, Amazon, Apple, Dell, Facebook,Google HP, IBM, Microsoft, Oracle, Tackspace, SalesForce, Twitter, Yahoo*) in base a vari fattori *(trasparency, infrastructure sting, Energy Efficiency and GHG Mitigation*, *Renewable Energy Investment*). La *company* più "virtuosa è *Akamai,* la peggiore, quanto in particolare alla *transparency*, è risultata *Twitter* (che qui non vuole, evidentemente, … cinguettare…) e che, inoltre, secondo il rapporto …*"has failed to set goals on how to reduce its obvlousy increasing emissions…"*[23]

23 A proposito dei gravissimi problemi climatici creati dalla "*dirty energy*", vedi l'articolo di A. CIACULLO dal titolo "*Ambiente – Quel patto sull'energia che può salvare il mondo"* in La Repubblica del 3/4/2012, nel quale si parla degli studi e delle previsioni catastrofiche per il prossimo futuro per ciò che riguarda i disastri ambientali e gli scenari politici (guerre scaturite dal caos climatico). Vedi anche l'articolo di V. GUALERZI dal titolo "*Stangata milionaria dal cambiamento climatico*" in La Repubblica, Affari e Finanza del 16.4.2012).
A proposito di clima e di CO_2, vedi l'articolo di DUSI dal *titolo "Clima – La sconfitta degli scettici del riscaldamento globale"* in La Repubblica del 11 aprile 2012 secondo cui i ricercatori di Harward hanno ricostruito gli eventi che portarono alla fine dell'era glaciale e dimostrato il rapporto causa-effetto tra l'aumento dell'anidride carbonica e quello della temperatura e quindi lo stretto legame tra il gas serra e il mutamento climatico.

Può concludersi affermando che in genere quasi tutte le compagnie interessate non eccellono in tema di "*transparency*", essendo piuttosto reticenti quanto alle informazioni relative ai loro dati. Tale mancanza, puntualizza il rapporto, *"...is not due to fact that data not existe..."*[24]

A proposito di tutela dell'ambiente rilevo ora che il *paper* del Garante per la protezione dal titolo "*Could computing: indicazioni per l'utilizzo consapevole dei servizi",* espone ampiamente i pregi e le utilità del ricorso alla *nuvola*, sia da parte delle organizzazioni private che pubbliche, non mancando, peraltro, di accennare ai potenziali rischi per i dati personali insiti nell'uso dei servizi *cloud-based* ed ai *caveat* relativi, e fornendo specifiche indicazioni per l'utilizzo consapevole dei servizi *cloud*. Tuttavia in questo *paper* manca, qualsiasi accenno ai rischi dell'espansione dei servizi *cloud* e all'inquinamento ambientale creato, allo stato, dall'uso della *dirty energy* per il funzionamento delle grandi *farms*, argomento questo peraltro inevitabile a mio sommesso avviso, allorché ci si proponga di esaminare i benefici ed i rischi[25]

24 Secondo recentissime notizie di stampa (vedi l'articolo dal titolo *"Una nuvola pulita per le future città smart"* di A. GRANELLI, in Corriere delle Comunicazioni del 7 maggio 2012) a seguito delle campagne promosse da *Greenpeace, Facebook* avrebbe costruito una *solar farm* per alimentare i propri *servers* in Oregon e starebbe progettando un nuovo *"data center"* in Svezia, mentre *Apple* avrebbe replicato alle accuse, sottolineando l'investimento miliardario in energie pulite per coprire il fabbisogno del *data center* in North Carolina. *Greenpeace* ha però replicato, osservando che i progetti di espansione del Centro in questione contemplano un raddoppio del parco *server* e quindi dei suoi consumi…

25 Il piano di *e-government* 2012, preparato dall'ex ministro Brunetta, prendeva in considerazione, tra i suoi obiettivi settoriali(n.8) ,anche l'ambiente, prevedendo,a proposito della efficacia energetica (in generale) degli apparati, di".. *ridurre gli sprechi nel consumo di energia delle amministrazioni pubbliche*

collegati all'uso nei nuovi servizi. Certo è strano che la medesima "cecità" per i sopracitati rischi ambientali si riscontri in altro *paper* del Garante, intitolato *"Smartphone e tablet: scenari attuali e prospettive operative"* nel quale, pur citandosi l'uso del *cloud*, ed elencandosi i rischi, l'orizzonte appare sempre ristretto agli ormai ben noti pericoli per la *privacy.*

6) LA SICUREZZA DEL CLOUD COMPUTING.GLI ATTACCHI DEGLI HACKERS ED I BLACK-OUT DEI SISTEMI

Gli studi e le indagini eseguiti in vari paesi in tema di criminalità informatica, hanno mostrato una sua notevole espansione... In un recente studio statunitense dal titolo "*Blue Coat System 2012- Web Security Report*" si afferma che i *malicious sites* hanno subito un aumento del 240% nel 2012 e l'acquisto *online* di tecniche illegali è diventato ancora più semplice. Le *malnet infrastructure* rendono

---

attraverso un sistema di controllo basato su una rete di sensori..." Ovviamente nel documento non vi è alcun richiamo specifico al tipo di alimentazione dei *servers* pubblici ed al loro consumo. In tema di energie rinnovabili ,vedi il *paper* dal titolo "*Energie rinnovabili ed efficienza energetica*, Rubettino editore, 2012.

Potrei sbagliarmi, ma non mi risulta che i Ministri interessati alle strategie d'azione ambientale per lo sviluppo sostenibile in Italia ed alla strategia energetica nazionale (Ambiente e Sviluppo economico) abbiano mai preso in considerazione i problemi relativi all'impatto ambientale del *cloud computing.*

Va ricordato ora che esistono due importanti progetti sostenuti dalla UE con il contributo italiano cui partecipa *Alcatel-Lucent* per la riduzione dei consumi energetici del 50% nel breve termine e dell'80% nel giro di 3 anni per le reti mobili a parità di traffico e di tipologia di servizi (*econet-low energy consuption networks e geyser,* che mira alla realizzazione di reti di nuova generazione, di particolare interesse nei progetti *cloud* (vedi l'articolo dal titolo *"Alcatel-Lucent: verso una rete mobile più efficiente"* in *http://www.inctbusiness.it.cont/news/alcatel-lucent)*...

possibile ai cybecriminali di lanciare attacchi dinamici, che spesso non sono individuati dai tradizionali produttori di antivirus per giorni o addirittura per mesi… Gli *Web advertisement* (si tratta di una forma di promozione che usa Internet e il World Wide Web per mandare messaggi di *marketing* ed attrarre i clienti) sono diventati uno dei più insidiosi vettore degli attacchi.. Nel 2011 si è anche verificata una rivitalizzazione degli *spam* come strumento di attacco… Le minacce ,come affermano gli esperti, non provengono più da *hacker*s isolati che agiscono prevalentemente per scopi personali di notorietà ma rappresenta un *business,,* sempre più esteso, di organizzazione criminali che agiscono per fini economici. Tra i più temibili gruppi di criminali informatici vi sono i cosiddetti "*Heavyweig*" che sarebbero, secondo il Corriere delle Comunicazioni (vedi l'articolo dal titolo "*Hactivist, eMugger e Ninja"* del 14 marzo 2012) dei veri professionisti, membri della criminalità organizzata. L'obiettivo sarebbe-secondo il periodico-quello di "scippare" i dati sensibili delle aziende per poterli vendere al miglior offerente. Ci sarebbero due diverse categorie all'interno di questo gruppo, il primo con obiettivi a lungo termine che utilizzano gli *Advanced Persistent Threat*, e il secondo ,agente a breve-medio termine, per ottenere denaro I timori peggiori riguardano attacchi alle infrastrutture critiche, *in primis* le reti energetiche. Ha dichiarato in proposito Jean Armold, capo delle

politiche energetiche presso la Commissione Europea ″... *l'evoluzione delle reti elettriche in smart grid impone nuove modalità di protezione delle infrastrutture stesse: non si potrà non tener conto delle attività del cyberterrorismo, considerato che i dati viaggiano sulle reti informatiche e che le infrastrutture vengono gestite via software*…" (vedi l'articolo di C. Licata dal titolo " *SoS UE sul cybercrime*…" in Corriere delle Comunicazioni, numero 2 del 7 febbraio 2011). Secondo il Commissario Europeo agli affari interni, *Cecilia Malmstrom*, il *cybercrime* minaccia seriamente l'economia europea: pertanto è stato deciso a livello comunitario la creazione di un Centro Europeo per la lotta alla criminalità informatica che inizierà la sua attività all'Aja nel 2013 (vedi, al riguardo, l'intervista della Malmstrom, resa al Corriere delle Comunicazioni, numero 8, del 7 maggio 2012.) Ritornando ora all'argomento del cloud computing, come già accennato in precedenza, uno dei punti deboli della "nuvola", quello che suscita uno dei maggiori timori o comunque una delle maggiori perplessità dei futuri utenti del sistema, certamente riguarda la sicurezza[26]. Gli incidenti già avvenuti

26 In realtà, come osserva lo *Special Report* di Info World del gennaio 2011 dal titolo *Cloud Security Deep Dive*, … il *cloud* richiede *"A new security model for a new era"* giacché *"Cloud Security changes everything"*. Ed infatti l'organizzazione della sicurezza nel redigere il piano di difesa dovrà tenere conto di vari parametri e cioè: *"If dound responsible for security breaches, a company can be held liable if its computers are used as part of the botnet to hack into websites, disrupt communications via DoS attacks, share pirated files or attack machines with hacker scripts"*.

hanno avuto una risonanza mondiale e prodotti danni economici, a volte molto gravi[27].

Le semplici possibilità di attacco sono state illustrate, in un convegno di *hackers* (DEFCON 18) svoltosi a *Las Vegas* nel settembre 2010, da parte di due giovani consulenti in materia di sicurezza con una presentazione dal titolo terrificante "*Cloud Computing. A Weapon of Mass Destruction*?", mostrando come… *"by spending $ 6 with a credit card, that could have stolen, to deploy a simple computer program on a few virtual servers in the Amazon EC2 cloud, they were vable launch a DDS attack that took a small financial service company, their client, off the internet for a long time"*. Uno dei due presentatori ha concluso che *"With the help of the cloud, taking down small and midsize companies – networks is easy…it's essentially a town without a sheriff…"* Si tratta di un problema indubbiamente serio giacché… *"many sites built with social media and content management services or software are run on public cloud infrastructure and can lead a variety of cloud security problems…"* In definitiva, il ricorso al

27 Come posto in luce da alcuni autori (vedi il capitolo *Cloud Computing e protezione dei dati personali* redatto da L. BOLOGNINI ed altri nel volume collettaneo dal titolo *"Next Privacy"*, Milano, 2011 *... "Né sono trascurabili gli aspetti di natura geopolitica e militare connessi allo sviluppo del modello cloud. Esso, infatti, si regge su un'infrastruttura informatica robusta: perché funzioni sono necessari server e banda larga. I server in questione potrebbero essere oggetto di attacchi terroristici. Pensiamo a che cosa accadrebbe se una qualunque organizzazione terroristica riuscisse a sabotare o distruggere i server del governo statunitense, o quelli della F<ed o della BCE. Pensiamo se qualcuno prendesse di mira gli archivi sanitari di questo o quello Stato, ovvero quelli di un'importante casa farmaceutica che compie ricerche ed esperimenti su malattie ad alto potenziale epidemico…"*.

cloud computing consente ai SMBs un certo risparmio, ma, come afferma l'articolo *"...it comes a potential for unpredictable problems that can be very costly to fix and, in some extreme cases, can even kill a company..."*.

In realtà gli esempi di attacchi non mancano. I più noti riguardano il crollo di applicazioni come Amazon EC2 *(Elastic Cloud Computing),* fiore all'occhiello della Company, e di Sony (*Play Station Network*) i cui servizi, basati sulla "nuvola" sono andati in tilt, il primo per quattro giorni, il secondo addirittura per sei. Ciò ha rappresentato una severa mazzata *sull'hi-tech* e sul cinico ottimismo dei venditori del sistema in questione. Non soltanto, infatti, i giocatori di tutto il mondo hanno battuto la testa al muro ma molte decine di società hanno subito il blocco dei loro servizi[28].

Il crollo di Amazon EC2 iniziato il 21 aprile dello scorso anno, ha avuto anche come conseguenza, sia detto per inciso, la perdita irrecuperabile di alcune informazioni contenute sul *server* della piattaforma di *storage* remoto…, e sembra abbia recato seri problemi ad alcune applicazioni quali il monitoraggio di pazienti con problemi cardiaci[29].Ma i guai di Amazon non sono finiti…mel mese di giugno,come affermato nell'articolo dal titolo" Amazon Web Services,i bug dopo la tempesta (hptt://www.news.it), in seguito ad una tempesta che ha colpito il nord della Virginia, sono

28 *".*

stati interrotti i servizi offerti da Netflix,Instagram e Pinterest… La mala sorte si è accanita contro l'impresa giacchè un *bug* inatteso ha colpito le istanze ELB (Elastic Load Balancer) che distribuiscono tra le diverse istanze EC2 il traffico diretto ad un indirizzo IP..un altro bug ha impedito anche il ripristino automatico dei *backup* di alcuni data base …Secondo l'articolo citato ,l'accaduto ha costretto,ancora una volta, ad una riflessione sull'attuale consistenza della "nuvola" e sui servizi che vi si affidano…

Per quanto riguarda, invece, il blocco della *Playstation Network* di Sony, la società ha ammesso l'esistenza di un grave attacco *hacker* ed il fatto che sarebbero stati sottratti o comunque compromessi i dati degli utenti del servizio[30].

---

29 Come ricorda V. MACCARI nell'articolo di commento apparso in Affari e Finanza del 3 maggio 2011, gli episodi sopracitati sono stati certamente i più gravi ma non sono gli unici, essendo stati preceduti da altri, sia pure meno gravi. Così, ricorda ancora MACCARI, nel 2008 una serie di brevi *black-ou*t ha sospeso il funzionamento di *Gmail*. Nel 2009 la texana *RackSpace* è stata costretta a rifondere 2 miliardi e mezzo di dollari ai suoi clienti a causa di un *outage* di un giorno intero. Nello stesso anno, ad ottobre, un altro *black-out* dei servizi *cloud* ha colpito gli *smartphone* Siderick di Microsoft, rischiando di cancellare i dati personali di 800mila utenti. Incisive le frasi pronunciate a commento dal V.Presidente della ricerca di *Gartner* e riportate testualmente dall'articolista "*…Le persone adesso realizzeranno che il cloud computing non è "magico" come pensavano e che non garantisce per forza la continua disponibilità dei servizi informatici".*
In argomento vedi anche l'articolo di G. CARRISI dal titolo *"Cloud, istruzioni per un 'buon uso'",* in Corriere delle Comunicazioni, febbraio 2012 e l'articolo di V. FREDIANI dal titolo*"Cloud e "Nuvole""*, in *http://punto-informatico.it/3426869/PI/Commenti/cloud-nuvole-aspx*.

30 Anche la stampa periodica si è occupata della sicurezza del *cloud computing*, così E. Manacorda in un articolo di volgarizzazione del *cloud computing* (*Il Futuro sulle nuvole*, in L'Espresso del 11 agosto 2011), sia pure rifacendosi ad uno studio del *Ponemon Institute* dal titolo *Security of Cloud Computing Providers*,ha richiamato l'attenzione sui pericoli relativi alla sicurezza ed alla *privacy.* Vedi anche l'articolo di L. Mannella dal titolo *"Aiuto, arrivano gli hackers",* in L'Espresso del 12.8.2011. Vedi in argomento *"The benefit of basing email and web security in the cloud*", un *White Paper* della Bloor Research. In argomento vedi anche della *Realtime Publishers* il recente *paper* dal titolo *"Web Security Services: Delegating Security Responsibility to the Cloud",* di Mike Danseglio.

Ma anche in Italia non si scherza quanto ad incidenti: vedi al riguardo il rogo di Arezzo della *web farm* di Aruba e l'articolo di Bocci-Montanari dal titolo "*Rogo nella cassaforte del WEB in tilt siti e mail di mezza Italia"*, in La Repubblica del 30/4/2011[31].

In tema di sicurezza del *cloud computing* vedi, in argomento, l'articolo di E. CALAMARI dal titolo *Cassandra Crossing/Le nuvole minacciose di Internet*, in Punto Informatico del 11/2/2011 e, dello stesso autore, l'articolo dal titolo *Cassandra Crossing/Il Cloud e me*, in Punto Informatico del 18/2/2011.
Circa la sicurezza del *cloud*, vedi l'intervista resa da C. Bonomi, Presidente del Gruppo Terziario Associativo (?) di Assolombarda al periodico Corriere delle Comunicazioni del 14 novembre 2011: al riguardo l'intervistato, apoditticamente,ha dichiarato… *"Oggi i dati sono più sicuri se collocati in un server cloud che in data base tradizionale…".*

31 Le gravi conseguenze anche a livello internazionale di un *black-out* sono apparse chiaramente a mezzanotte di venerdì 28 gennaio 2011 allorché l'Egitto è uscito da Internet. Come afferma l'articolista L. CASTELLI *"... da un minuto all'altro, in un gigantesco blackout informatico, tutte le connessioni che tenevano collegato il Paese al Web sono state staccate..."* (in La Stampa del 29/01/2011).Per quanto riguarda il nostro Paese va ricordato che i *black-out* di Poste italiane sono ormai storici… nel gennaio 2003 il più clamoroso. Un *virus*,lo SQ Hell, peraltro preannunciato dagli esperti, mise in ginocchio l'intera rete, (14mila uffici postali in tutta Italia), favorito, sembra, da un mancato aggiornamento dei programmi informatici degli uffici postali… Altro "botto" si è avuto nell'ottobre dello scorso anno nel quale, per cause non precisate, di nuovo è andata in tilt l'intera rete delle Poste, creando, secondo la stampa (vedi in La Repubblica del 18/10/2011, l'articolo dal titolo *"Poste, nuovo blackout . Cisl: sciopero nazionale*") gravi problemi, soprattutto in Sardegna regione nella quale scadeva il termine per presentare le domande di contributo al progetto di imprenditorialità "*Impresa Donna*", ed inducendo l'arrabbiatissimo Segretario Generale della CislPoste a minacciare uno sciopero nazionale di protesta… Ma si vede che l'Ente è proprio disgraziato… o forse esiste qualche jettatore interno…sta di fatto che un altro *black-out* nazionale si è verificato il 17/4/2012, tanto grave da indurre il furibondo Segretario Generale di CislPoste, interprete del disagio generale, a sollecitare un intervento della magistratura per individuare eventuali responsabilità, dichiarando, tra l'altro, alla stampa, fuor dei denti *"... ci sembra scandaloso che continuino a verificarsi episodi simili, dal momento che il sistema operativo è costato milioni di euro. Ed è grave che l'azienda non si sia dotata di un piano di emergenza!"* (vedi in La Repubblica del 17/4/2012 l'articolo dal titolo *"Uffici postali in tilt, code ed esposti").*La situazione ha spinto il senatore Lannutti a rivolgere, in sede di Sindacato Ispettivo (Atto n 4-07310 del 18 aprile 2012..) una durissima interpellanza al Ministro dello sviluppo economico, adombrando. tra l'altro, delle irregolarità da parte dell'alta dirigenza di Poste Italiana nella stipula dei contratti con l'IBM per la informatizzazione degli uffici postali, e chiedendo espressamente "*…quali iniziative il Governo intenda intraprendere al fine di fare luce sui perenni disservizi di una azienda pubblica, come Poste Italiane, anche al fine di individuare eventuali responsabilità della continua interruzione di un pubblico servizio.."* Dati questi precedenti,notevole sorpresa.accompagnata da caustici commenti degli esperti,,ha suscitato la notizia secondo cui l'AD delle Poste italiane,Sarmi, si è recato in Russia per attuare una *liason* digitale con Russian Post allo scopo di pianificare lo sviluppo e l'ammodernamento della rete logistico-postale russa ,il restyling tecnologico degli uffici postali e l'introduzione di servizi ad alto valore aggiunto ,attività possibili,,ha affermato l'AD italiano "*…grazie alla tecnologia e all'infrastruttura fisica e tecnologica di Poste Italiane.."* (Il Corriere delle Comunicazioni,news del 24 luglio)… Forse i dirigenti di Russian Post ignoravano i problemi tecnici che affliggono le Poste italiane,vai a sapere…

In tema di sicurezza va ricordato che la sicurezza del *cloud computing* è una delle preoccupazioni del Governo USA. Il NIST *(National Institute of Standards and Technology)*, una agenzia del *Commerce Department's Technology Administration*, ha creato un *Cloud Computing Security Group* per determinare il modo migliore di assistere le agenzie che desideravano adottare il *cloud computing*, soprattutto per quanto riguardava i rischi relativi all'adozione della nuova applicazione. In argomento va ricordato che anche un selezionato gruppo industriale, a novembre 2011, ha rivolto alla Commissione Europea dieci raccomandazioni circa l'orientamento della strategia europea del *Cloud Computing*.

I principali *items* del rapporto sono:

1) *Data Privacy, Governance and Identity;*
2) *Trust, Security and Certification;*
3) *Interoperability, Data Portability and Reversibility;*
4) *Innovation and Uptake;*
5) *Key, Recommendation and Action.*

In materia di sicurezza, importante è anche il *paper* del marzo 2010 dal titolo *"Top Threath to Cloud Computing V 1.O"*

Con una certa disinvoltura,peraltro, ,l'amministratore delegato di Poste Mobile,R-Giacchi, si è presentato al solito Forum PA di quest'anno per illustrare una" nuova gamma di soluzioni basata sull'integrazione con la SIM per usare il cellulare come titolo di viaggio", dichiarando …" **Puntiamo a semplificare la vita ai cittadini**…"Immaginabili al riguardo i i commenti dei cittadini vittime dei blackout, e soprattutto dei poveri pensionati, flagellati dai sopra citati ripetuti black-out !!

preparato dal *Cloud Security Alliance* che analizza le seguenti minacce:

1) *Abuse and Nefarious Use of Cloud Computing;*
2) *Insecure Application Programme Interfaces;*
3) *Malicious Insiders;*
4) *Shared Technology Vulnerabilities;*
5) *Data Loss/Leakage;*
6) *Account, Service and Traffic Hijacking.*

Altro studio molto importante statunitense in tema di sicurezza è quello dal titolo *"State of Internet 2010. A Report on the Everychanging ThreatLanscape"* eseguito dalla *CA Technologies Internet Security Business Unit (ISBU)* nel quale si parla di un meccanismo *underground market,* che il rapporto chiama *Crimeware-as-a-Service*. e che si riferisce a" minacce modulari", designate per eseguire specifici compiti. Tali minacce lavorano insieme, allo scopo di creare un *crimeware ecosystem* , prendendo per modello il sistema del *cloud computing*. Più particolarmente, secondo il rapporto, *crimeware* è una classe di minacce designate per automatizzare il *cyber crime*: esso raccoglie informazioni sensibili mediante *"a large-scale malware infections"*. Il suo scopo primario è quello di sottrarre dati e compiere *"identity theft"* per accedere ai conti di utenti di servizi bancari online, attuare

"shopping transactions", ecc. In definitiva il *crimeware* può definirsi come *"a cloud-enabled threat"*!!

Il rapporto elenca poi alcuni esempi notevoli di *"abuse of cloud service".* Il primo riguarda il *Google Group*, rivelando che nel maggio 2010 la sopracitata *CA Technologie (ISBU)* ricevette una *"malicious spam campagn",* usando proprio il servizio che supporta il gruppo di discussione *Google Group*, allo scopo di ospitare un attacco *email* fraudolento. Nel settembre 2009 un *Trojan*, individuato come *Win32/Grupbot A*, era contenuto in uno *spot*, destinato in realtà a distribuire comandi e funzioni di controllo fraudolenti, usando proprio *Google Group*.

Circa i servizi di *Amazon* EC2, il rapporto rivelava che nel dicembre 2009 una *"spam campagn",* spargente una notevole variante di *Zeus Bot*, era stata scoperta come avvalentesi dei servizi di cui sopra per acquisire comandi e controlli di funzionalità. Il *"Twitter Spam",* invece, si riferisce ad una *"spam campagn"* condotta come una *email notification*, proveniente apparentemente da insospettabili utenti di *Twitter* e di *You Tube*, ma contenente in realtà immagini pornografiche aventi lo scopo di indurre il soggetto preso di mira ad accedere ad un sito Web manipolato, ospitante *"a drive-by download attack".*

Non vi è dubbio che l'adozione del *cloud* richieda una strategia *ad hoc,* ed, in particolare, l'adozione di procedure di sicurezza più

sofisticate, per così dire, rispetto a quelle adottate nell'area degli ordinari servizi internet, insieme ad una competenza e formazione maggiore da parte del *management*, anche in tema di *data recovery.*

Anche i *bugs* ,infatti,fanno la loro parte nel danneggiamento dei sistemi. Come affermano alcuni autori (vedi il già citato capitolo dal titolo *Cloud computing e protezione dei dati personali*, redatto da I. Bolognini ed altri,) negli ultimi due mesi dell'anno 2010 due importanti *defiance* hanno colpito *social networks* come *Facebook* e *Google Docs*… il primo ha visto sparire istantaneamente le foto di 15 milioni di iscritti mentre il secondo, un servizio che consente di creare, modificare e condividere *online* i propri documenti, ha visto il *bug* colpire i privilegi di accesso, rischiando in tal modo di rendere pubblici migliaia di documenti privati giacché lo scambio di dati non era automaticamente protetto dal protocollo di sicurezza *https.*

I rischi derivanti per il *cloud computing* dall'uso dei *Botnets* (secondo Wikipedia, si tratta di una rete formata da computer collegati ad internet infettati da *malware* e controllata da una unica entità ,il *botmaster*) come afferma un recentissimo *paper* di *SOPHOS*, una importante società di sicurezza informatica USA, redatto dal *Senior Product Manager* A. Comazzetto, dal titolo "Botnets: The dark side of cloud computing", sono costituiti dal

fatto che *"...Botnets rival the power of today's most powerful cloud computing platforms... these "dark" clouds, controller by cybercriminals... are designed to silently infect the network... left undecteded, botte borrow the network to serve malicious business interest..."* In definitiva, quindi, i *botnets*, secondo il *paper* citato *"...pose a significant threat to business, randomly attacking vulnerable computers or nodes without being traced back to an operator..."* Il *paper* in questione mette in guardia, tra l'altro, anche in relazione ai rischi legali scaturenti da negligenze nei sistemi di sicurezza delle organizzazioni.

In tema di sicurezza va ricordato che anche il Commissario Europeo per l'Agenzia Digitale, *Neelie Kroes*, ha più volte messo in guardia relativamente ai rischi per i dati personali derivanti dal *cloud computing*. Nel suo discorso alla conferenza "*Les Assises du numerique*" svoltosi a novembre del 2010 *all'Université Paris-Dauphine* , ha dichiarato che il *cloud computing* è più di una semplice sfida tecnologica. C'è infatti il rischio-ha affermato *Kroes*- di perdere il controllo dei dati personali una volta che questi finiscono in *servers* remoti .

Al momento, il più interessante studio sulla sicurezza del *cloud computing* in area privata sembra essere quello condotto dal *Ponemon Institute*, (nota società statunitense dedicata alla ricerca indipendente, il cui compito è quello di *"... to conduct empirical*

studies on critical issues affecting the management and security of sensitive information about people and organisation"). studio sponsorizzato dalla *CA Technologies*, una società di software e soluzioni per la gestione dell'IT.Lo studio in questione (che fa seguito ad altri precedenti) dal titolo *"Security of Cloud Computing Providers Study",* pubblicato nell'aprile 2011, è fondato su interviste eseguite a 103 fornitori di servizi di *cloud computing* in USA e ad altri 24 fornitori residenti in 6 Paesi europei, per un totale di 127 fornitori. Secondo lo studio in questione :

a) la maggioranza dei providers intervistati non ritiene che le loro organizzazioni considerino la sicurezza come un vantaggio competitivo;

b) la maggioranza dei sopracitati providers ritiene che sia compito dei loro clienti rendere sicuro il *cloud* e quindi che la sicurezza non rientri nella loro responsabilità;

c) la maggioranza degli intervistati ha dichiarato di stanziare al massimo il 10% delle risorse IT per la *security* o per altre attività deputate al controllo;

d) in generale i providers intervistati ritengono che gli acquisti delle risorse del *cloud* da parte dei clienti *"...are lower cost and faster deployment of applications…";*

e) la maggioranza dei *cloud providers* ammette di non aver destinato personale specializzato in tema di sicurezza per controllare la sicurezza delle applicazioni *cloud*, delle infrastrutture e delle piattaforme;

f) i *providers* dei sistemi del *private cloud* attribuiscono più importanza alla capacità del loro personale nel raggiungere gli obiettivi di sicurezza rispetto ai *providers* delle soluzioni *cloud* ibride e pubbliche.

Lo studio conclude affermando che "…*The key finding in this study is that providers of cloud computing resources are not focused on security in the cloud. Rather, their priority is delivering the features their customers want such as low cost solutions with fast deployment that improves customer service and increases the efficiency of the IT function. As a result, providers in our study conclude that they cannot warrant or provide complete assurance that their products or services are sufficiently secure."* Un altro paper dell'IBM dal titolo " *Cloud Security.Who do you trust* ? ", dell'ottobre 2010 , esamina le sfide per le imprese nella introduzione del *cloud e*d indica la scelta migliore,a suo avviso,per la singola impresa…Inn argomento va citato anche un recente paper della Intel dal titolo" *Planning Guide -_Could Security* ",contenente informazioni pratiche per aiutare le imprese ad

integrare il piano della *security* nelle iniziative relative al cloud computing

7) CENNI SUI RIFLESSI GIURIDICI DELL'USO DEL CLOUD COMPUTING

Nel settore processualistico penale ci si è chiesti se il ricorso al *cloud computing* possa rendere difficile o addirittura impossibile acquisire la prova dei reati. Secondo l'esperto giudiziario francese *S. Migayron*, (vedi l'intervista resa ad *Expertises* ,n. 354 del gennaio 2011,), nel *cloud* il *log* potrebbe divenire un mezzo privilegiato di accesso alla prova. Secondo l'esperto in questione i problemi quindi ci sono… *"mais si on dispose des logs de confiance conçu comme elements de preuve, alors des investigations lourdes e coûteuses pourront être évitées…"*

Il ricorso al *cloud computing* comporta anche importanti problemi civilistici per quanto riguarda la contrattualistica, la responsabilità ed il trattamento dei dati nell'ambito dei vari servizi forniti. Per quanto riguarda in particolare l'ultimo argomento occorre assicurare tracciabilità e sicurezza dei flussi. Come osserva l'esperto francese Jerome Debras nell'articolo dal titolo *Aspects juridique de la contractualisation de la forniture de service e du traitements des données, (*in *Expertises,* n.354 del gennaio 2011)"… *Le choix du pays dans lequel est réalisé l'hébergement*

de données ou la simple transmission d'un flux est essentiel a la sécurité des données. Au-delà de l'aspect tehnique, c'est la sécurité d'un ordre juridique donné qui peut être ou non facteur de confiance et rassurer un client sur le cas hypothétique d'une nécessité de sauvegarder ses droits en justice"[32]. Occorre ora precisare che, non esistendo al momento una regolamentazione giuridica specifica per il *cloud computing*, il problema si sposta sul terreno dottrinario.. e riguarda il possibile inquadramento dell'applicazione nel sistema giuridico vigente. Secondo Belisario (vedi l'articolo dal titolo "*Cloud Computing: quale legge sulle nuvole*?" in Nuove Tecnologie del 18/2/2011) il contratto di fornitura di servizi c*loud* integra una specie di appalto ,avente ad oggetto prestazioni continuate o periodiche. In relazione alla legge applicabile ed al foro competente, l'autore afferma che… *"In assenza di una normativa che individui sempre chiaramente la legge applicabile, bisognerà verificare che il fornitore indichi in quale Paese sono situati i server che ospitano i dati; per l'utente è importante sapere se eventuali controversie potranno essere decise*

32 Vedi anche l'articolo di BENJAMIN JACOB dal titolo *"Cloud Computing. Les points clès des contrats*", in Expertise del marzo 2011. Anche una analisi di *Gartner* rileva la scarsa trasparenza dei contratti *cloud* e la mancanza di protezione dell'utente di fronte alla forte posizione del *provide*r (vedi al riguardo l'articolo di P. LICATA dal titolo *"Cloud, contratti inadeguati",* in Corriere delle comunicazioni n. 5 del marzo 2011, e l'articolo di D. GOMEZ dal titolo *"Cloud Computing survey finds issues with some contracts"*, in http://www.tgdaily.com/networking-features/52707... che riporta i risultati di una indagine compiuta dalla citata *School of Law* della *Queen Mary University of London*, secondo cui *"... many contract have clauses that could have a negative effects on the rights and concerns of customers..")*

dal giudice italiano piuttosto che da un giudice straniero (con l'ovvio aggravio di costi). La collocazione fisica del server è importante anche in relazione alla possibilità di ottenere l'esecuzione dei provvedimenti ottenuti dal giudice italiano (senza bisogno di complessi procedimenti) oltre che sotto il profilo dell'autonomia del fornitore rispetto all'ingerenza dei pubblici poteri e al grado di democraticità di questi ultimi".

Anche altri pubblicisti italiani hanno cercato di inquadrare il *cloud computing* nel sistema giuridico vigente.

Secondo S. Benandi, (*Software as a Service (Saas): aspetti giuridici e negoziali,* in *www.stefanobenandi.com/software-as-a-service-aspettigiuridici),* 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 propria e al pagamento di un compenso, sono tutti elementi che farebbero propendere per la configurabilità di un "appalto di servizi" sia pure avente ad oggetto prestazioni continuative o periodiche. Rilevo però che se si accetta questa tesi, occorre tener presente la regolamentazione della contrattualistica nel settore pubblico per la scelta del *provider.*

Secondo altra tesi[33], sarebbe da escludere la natura di appalto di servizi in quanto si tratterebbe invece di un contratto atipico:..s econdo altri saremmo in presenza di un contratto di adesione, data la predisposizione rigida del modello contrattuale da parte del *provider.*

Un interessante studio di analisi e di confronto legale dei contratti relativi ai servizi *cloud* offerti agli utenti è stato fatto, come già detto alla nota 28, dalla *Queen Mary University of London, School of Law* nel 2010 (vedi il *paper* dal titolo *Contracts for Cloud: Comparison and Canalysis of the Terms and Condition of Cloud Computing Services),* effettuato comparando 31 servizi offerti da 27 affidabili *providers*, scelti a campione tra gli USA e l'Unione Europea. Dal canto suo il Ministero tedesco dell'Economia e della Tecnologia ,ha pubblicato un interessante studio dal titolo" *The Standardisation Environment for Cloud Computing "*(www.trusted.cloud) nel quale rileva,tra l'altro, che la situazione normativa relativa alla standardizzaziione del cloud computing è,in generale,incerta o poco chiara.. Sela Commissione CEE si

33 Cfr. F. NICOLA, *I nuovi paradigma della rete. Distribued computing, cloud computing, computing paradigms:,* in *www.ddiritto.it/art.php?file=/archivio/27973.html* vedi anche R. FREATO-S. COSSINCARE, *SLA gli aspetti legali,* in *www.beccloud.it/*. Vedi, *amplius,* l'articolo di A. FUPU, A. TESSALONITOKOS, *La spécificités du contrat informatique relatif au software as a service (Saas),* in *Expertises,* settembre 2009, p. 308 ss., cui *add*e, H. CARADOU, *Le droit dans les nuages, ivi,* luglio 2010, p. 251 vedi anche ; *Above the cloud*, di autori vari, in *http://berkeleyclouds.blogspot.com* dell'11 giugno 2009; cui *adde , La révolution du cloud computing,* di P. DESMDT, in *www.usinenouvelle.com/article/la-révolution-du-cloud-computing*

appresta a pubblicare una comunicazione sulla strategia del cloud computing ,i cui pilastri sarebbero quelli della armonizzazione dei regolamenti nazionali,l'agevolazione del traffico tranfrontaliero dei dati e le condizioni contrattuali in tema di servizi cloud. Per concludere ora per quanto riguarda l'arcomento del *cloud computing*, devo dire che non mi sento di dare troppo torto alle critiche ed ai giudizi pesanti di *Ellison* e di *Stallman* In effetti è noto che le innovazioni tecnologiche si prestano benissimo a grosse operazioni di *marketing*: non appena appare infatti una nuova tecnologia informatica o una nuova applicazione, alcune grandi imprese, specie multinazionali, si lanciano all'assalto del mercato. Strategie e tattiche sono le consuete… i soggetti del *management* e quelli delle pubbliche relazioni elaborano articolate strategie mediatiche, cercando anche, nell'ambito di un particolare programma di penetrazione, di individuare nel settore privato, ma specialmente in quello pubblico, i possibili *decision makers* (tecnici, burocrati e politici) competenti per quanto riguarda la scelta e l'adozione delle nuove tecnologie e per gli acquisti relativi. Una volta individuati tali soggetti li si contattano e li si corteggiano, cercando di creare in tutti i modi una specie di "aggregazione culturale". Seguono poi pseudo convegni scientifico-culturali ai quali vengono invitati i soggetti, soprattutto istituzionali, che si presume convertiti o convertibili...

In pratica i problemi, quasi sempre esistenti, relativi principalmente alla sicurezza delle innovazioni ed alla tutela dell'ambiente e della *privacy*, vengono disinvoltamente ficcati "sotto il tappeto", ignorati o minimizzati: naturalmente vengono viste come vere "bestie nere" gli esperti indipendenti che cercano, veri *Grilli Parlanti*, di aprire gli occhi ai possibili acquirenti per quanto riguarda i pericoli concernenti la sicurezza e la *privacy* nell'uso e nella gestione dei prodotti. Questo, sia detto per inciso, si è puntualmente verificato in Italia per quanto riguardava l'introduzione del Voip, del *RFID*, del WiFi, delle applicazioni biometriche nell'ambito delle P.A. ed ora si sta verificando, , anche per la promozione del *cloud computing* e per la sua adozione nel settore pubblico. 8) L'AGENDA DIGITALE ITALIANA ED I SUOI RIFLESSI SUL CLOUD COMPUTINING Il Governo, con il decreto-legge numero 5 del 9 febbraio 2012, convertito nella legge 4 aprile 2012 numero 35, all'articolo 47, intitolato "Agenda Digitale Italiana", al comma secondo ha previsto la istituzione di una "cabina di regia" per l'attuazione della detta Agenda[34]. Gli

34 Circa l'istituzione della sopra citata Agenzia, vedi i rilievi critici dell'ex Presidente del CNIPA, Zoffoli, contenuti nell'articolo dal titolo" *Agenda Digitale: Zoffoli: "serve un commissario straordinario*", in Corriere delle Comunicazioni del 6 maggio 2012. Ma anche critico circa l'Agenzia è l'ex Ministro Brunetta che in una intervista rilasciata il 22 maggio 2012 al Corriere delle Comunicazioni (vedi l'articolo di F.Mc. dal titolo "Brunetta: Agenda Digitale? Solo chiacchiere")..Altre critiche sono arrivate dal Presidente di Assitel,Avenia, secondo cui …"*la governance è ancora poco chiara:è necessaria una figura unica per guidare la rivoluzione digitale e risolvere i problemi tecnici*…" (vedi il Corriere delle Comunicazioni,del 22 maggio 2012).

obiettivi di una cosiddetta “cabina di regia” sono fissati nel successivo comma che prevede alla lettera d)*"... la promozione della diffusione del controllo di architetture di cloud computing per le attività e servizi delle pubbliche amministrazioni..."*

Non sappiamo se per quanto riguarda questo *item* sia stata disposta dal Governo la preventiva audizione di autentici ed indipendenti esperti del settore e, nel caso, se questi abbiano fatto presente al Presidente del Consiglio l'impatto sulla pubblica amministrazione della innovazione, in termini di costi economici ed organizzativi, e se gli abbiano fatto presente, i rischi della nuova applicazione e la necessità assoluta di ripensare *funditus* il problema della sicurezza dei sistemi vigenti, e quindi la necessità di rivolgersi a *providers* assolutamente affidabili in tema di specifiche garanzie ed in grado,tra l’altro di accollarsi le spese necessarie alla nuova sicurezza senza farle gravare sugli utenti . E’ noto infatti , e sempre sottolineato dagli esperti, che il *cloud computing*, in tema di sicurezza, richiede criteri **molto più stringenti** dell'ordinario. In definitiva, gli esperti avrebbero dovuto fornire al governo, in termini assolutamente chiari, gli elementi per valutare i costi-benefici dell'operazione.… Dato per scontato,per così dire che vi sia stato , l'interpello di esperti, c'è da chiedersi se questi abbiano fatto poi presente al committente che l'utilizzo delle energie

tradizionali per il funzionamento dei grandi *servers* , necessari per il decollo della trasformazione, avrebbe avuto un impatto ambientale inevitabile, posto che in tema di utilizzazioni di fonti naturali di energie il nostro paese non brilla… ed i previsti provvedimenti, anche in questo settore, non lasciano molte speranze… Va ricordato in argomento che nell'obbiettivo del Governo c'è un forte richiamo alla produzione della *"dirty energy*" e cioè al rilancio della produzione nazionale di idrocarburi…….. 9) IL "TORNADO" GOVERNATIVO IN TEMA DI INNOVAZIONE TECNOLOGICA

Le recenti notevoli iniziative del Governo nel campo della digitalizzazione e della innovazione tecnologica ed i suoi riflessi tecnici ed organizzativi , mi hanno indotto ad allargare il tema iniziale del presente articolo- In effetti ,esaminando le indicate

recenti iniziative governative, effettuate a colpi di decreti legge ,non può non rilevarsi, sia detto per inciso, che ,da una almeno una ventina di anni, i Governi che si sono succeduti in Italia hanno fatto ricorso fin troppo frequente ai decreti legge. Non ha fatto eccezione il Governo Monti, ricorrendovi in casi molto speciali, vedansi i recentissimi decreti legge " polpettone", tipo il DL 22 giugno 2012, n.83, relativo alle misure urgenti per la crescita del Paese che ha istituito, tra l'altro, come già detto, l'Agenzia per l'Italia Digitale, ed il DL 27 giugno 2012, n. 87,

dal titolo chilometrico, “Misure urgenti in materia di efficientamento (sic), valorizzazione e dismissione del patrimonio pubblico, di razionalizzazione dell’amministrazione economico-finanziaria, nonché misure di rafforzamento del patrimonio delle imprese del settore bancario …. Va detto ora che, non a caso, un articolo pubblicato dal giornale online “Punto informatico” del 6 luglio . dal titolo “I tanti nomi della PA digitale” sostiene che “… *la nuova Agenzia per l’Italia Digitale sembra solo l’ultimo espediente di un Legislatore che pare volere dissimulare la perdurante assenza di investimenti in tecnologie digitali nel Paese, mediante la creazione di organismi ed enti sempre nuovi e preposti al coordinamento di future iniziative in materia ,,*”. Uno degli argomenti più discussi da vari commentatori delle iniziative governative è stato quello della soppressione-accorpamento di vari enti (DigitPa, creatura -non rimpianta- dell’ex ministro Brunetta, e Agenzia per la diffusione delle tecnologie dell’innovazione). Soppressione effettuata, tra l’altro, mandando a casa, nell’operazione, (definita, irosamente , dagli interessati privati della seggetta “**Nacht und Nebel**”) ,senza tante cerimonie, il Presidente ed il Comitato Direttivo di DigitPA, ed altri alti dirigenti(i cui mugugni e lai sono facilmente immaginabili..,) e che ha suscitato, sia detto per inciso, anche le proteste dei Sindacati CGIL e CISL del settore. Per quanto

riguarda la raffica delle iniziative governative sopra citati, i commenti critici degli esperti sembrano concordare, in linea di massima , su vari punti e cioè che le operazioni di picconamento del Governo hanno dimostrato una certa scarsa conoscenza dei principi di scienza dell'amministrazione, una trascuratezza nella considerazione dei gravi problemi organizzativi e psicologici conseguenti alle demolizioni "a colpi d'accetta" e perfino, in qualche caso, evidenziato una qualche incoerenza nella redazione di parte dei due provvedimenti, difetti tutti che sono stati posti in luce,come già detto, vivacemente da vari esperti del settore e che saranno elencati sommariamente di seguito. Tanto per cominciare ,va esaminato il problema della Consip. Per quanto riguarda le sue competenze, va osservato che l'articolo 20, comma 3, lett.c) del DL n.83 ha trasferito alla Società alcune competenze del soppresso DigitPA , e cioè le funzioni di cui all'articolo 3, comma 2, lettera c) del decreto legislativo 1 dicembre 2009, n.177, limitatamente alla formulazione dei pareri sulla congruità economica e tecnica degli interventi e dei contratti relativi all'acquisizione dei beni e servizi informatici e telematici, al monitoraggio dell'esecuzione degli interventi e dei contratti suddetti, nonché le funzioni di cui alla lettera d) e quelle di cui al comma 3 del suddetto articolo. Al riguardo gli esperti (vedi l'articolo di F.Meta dal titolo "Agenzia digitale, tutti i nodi

della governance", in Corriere delle Comunicazioni del 6 luglio 2012) hanno sottolineato il rischio di sovrapposizione dei ruoli in quanto il decreto n.83, trasferendo alla società del Ministero dell'Economia la funzione valutativa, non ha tenuto conto che è la stessa Consip anche ad organizzare la domanda, essendo in capo ad essa la gestione delle gare pubbliche. Altra sovrapposizione, nota l'articolista, riguarda la gestione del Sistema Pubblico di Connettività e della la Rete Internazionale della Pubblica Amministrazione dove si verifica una sovrapposizione di funzioni tra Consip e Agenzia per l'Italia Digitale. Ma l'iniziativa realmente sbalorditiva,sotto l'aspetto della coerenza e della tecnica legislativa, la si ritrova nell'articolo 4 del decreto legge n. 87/2012,comma 7 che, inopinatamente,ha trasferito alla Sogei S.p.a le attività informatiche a supporto delle amministrazioni pubbliche, già affidate dalla Consip. A prescindere dalla considerazione che logicamente tale disposizione avrebbe dovuto essere inserita nel precedente decreto n. 83/2012, lì dove si parla della nuove competenze della Consip, sta di fatto che il motivo di tale "ripensamento-giravolta" è restato totalmente sconosciuto. Non vi è una sola parola al riguardo, neppure nella relazione al disegno di legge n.3382 di conversione del decreto n.87, presentato dal Governo al Senato il 27 giugno 2012. Questa circostanza ha spinto il noto esperto , G. Scorza, nell'articolo

dal titolo " Informatica pubblica a rischio paralisi", pubblicato nel periodico Il Fatto Quotidiano del 17 luglio, ad affermare , a proposito della sequenza dei due decreti legge "…*viene da pensare ad uno sdoppiamento di personalità* …" ed ha aggiunto "… *Nella sua foga normativa e totale assenza di visione prospettica specie sui temi della innovazione, in appena cinque giorni il Governo ha trasferito delle competenze che una Autorità gestiva da quasi un ventennio e le ha trasferite, in rapida sequenza a due distinti soggetti, creando una situazione di drammatica confusione che minaccia di paralizzare l'informatica pubblica in quelli che avrebbero dovuto essere – nelle promesse dello stesso Governo - i mesi della rivoluzione digitale italiana ...."*. In effetti, ha aggiunto ancora l'esperto, *"... La Sogei S.p.a, società di Information &Communication Technology del Ministero dell'Economia e delle Finanze, si ritroverà ad emettere i pareri di congruità sui contratti per l'acquisto di beni e servizi informatici da parte della intera pubblica amministrazione italiana*". L'articolista nota ironicamente , infine che "… *affidare alla Sogei il compito di congruità sui contratti che la pubblica amministrazione dovrà concludere in materia informatica è come affidare alla FIAT il compito di emettere i pareri di congruità sugli acquisti di autoveicoli da parte della pubblica amministrazione ..."* ed ha

concluso*"..... è una scelta drammaticamente sbagliata e sorprende che il Governo dei professori continui a commettere – sempre che di questo si tratti - ingenuità grossolane di questo livello…*". A proposito della Sogei, forse è il caso di ricordare, per inciso, che l'anagrafe tributaria, gestita dalla società in questione, dal punto di vista della sicurezza era, almeno fin a qualche tempo fa, una specie di colabrodo. Le indagini eseguite dalla magistratura e quelle amministrative dimostrarono la scarsa cura della società per i criteri di sicurezza dell'anagrafe tributaria allorché, nel 2006, vennero alla luce gli incredibili accessi abusivi, durati a volte anni, da parte di numerosi pubblici dipendenti (ben 127 quelli individuati!!) e perfino da parte di estranei alla pubblica amministrazione, ai dati fiscali di alte personalità (Romano Prodi, sua moglie Flavia , il Presidente Napolitano) e di altri politici sia di sinistra che di destra, di calciatori della Nazionale, di soubrettes e di noti managers. Lo scandalo indusse anche il Garante per la protezione dei dati personali al intervenire, l'anno seguente, eseguendo appositi accertamenti in tema di sicurezza per quanto riguardava gli accessi all'anagrafe tributaria, al termine dei quali, constatate varie irregolarità, emise una serie di precise prescrizioni (provvedimento del 18 settembre 2008). Detto per inciso, non si è mai avuta notizia di inchieste interne e di

responsabili della sicurezza messi alla porta . o quanto meno sanzionati disciplinarmente!!!.

Altro problema, ha rilevato la citata articolista F. Meda (Corriere delle Comunicazioni del 16 luglio), è quello delle scelte organizzative attribuite a ben tre Ministeri (MIUR, Sviluppo economico, Funzione Pubblica) e della attribuzione alla Presidenza del Consiglio dei compiti di vigilanza. Il problema, sostiene l'articolista, è che l'Agenzia potrebbe finire per divenire un luogo di concertazione tra dicasteri con il rischio di soccombere ai veti incrociati e quindi di replicare una frammentazione già vista nell' IT pubblico. Il rischio di una paralisi dell'informatica pubblica a seguito di alcune disposizioni dei citati decreti legge del Governo, è stato esposto, con molta chiarezza ed incisività, da G. Scorza nell'articolo sopra citato. Il trasferimento di competenze, in piena estate, ha osservato l'articolista, da un Autorità attiva da quasi un ventennio ad una nuova autorità ancora priva di vertici, uffici, organizzazione e personale, è stato un azzardo che ci si sarebbe potuto risparmiare!!

La ciliegina sulla torta è rappresentata da una disposizione contenuta nell'art. 21, comma 2, del Decreto legge n.83 a proposito degli organi dell'Agenzia per l'Italia Digitale. Si stabilisce, tra l'altro, che la stessa avrà a capo un Direttore Generale, che dovrebbe essere nominato **entro trenta giorni**

dall'entrata in vigore del decreto, dal Presidente del Consiglio dei ministri e da un *pool* di quattro ministri, **previo avviso pubblico**, si dice, tra "*..persone di particolare e comprovata qualificazione professionale in materia di innovazione tecnologica e in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione*" . Gli esperti si stanno rompendo il capo per risolvere il significato del termine criptico " **avviso pubblico** " giacché né sul sito della Presidenza né in quello dei numerosi ministeri coinvolti vi è una qualche traccia del citato avviso…. Si chiede, giustamente, l'esperto Scorza sopracitato, in un altro articolo dal titolo "*Nominopoli.ora tocca all'Agenzia per l'Italia Digitale*?" pubblicato nel Il Fatto Quotidiano del 12 luglio "…. *Che senso ha pubblicare l'avviso – e dunque invitare chi ritenesse di avere i requisiti a candidarsi – a pochi giorni dal termine ultimo per la nomina del direttore generale?".* L'esperto in questione, evidentemente ricordandosi di un famoso detto dell'immarcescibile Andreotti (*..a pensare male si fa peccato ma spesso si indovina ..*) non può trattenersi dall'affermare che è "*..Difficile respingere il dubbio che, ancora una volta, qualcuno abbia già deciso chi sarà il nuovo direttore generale …*" (al riguardo *radio fante* già indica un paio di nomi …) e conclude, con un preoccupante *caveat "... Sarebbe davvero grave, tuttavia, se il Governo dei Professori, a*

poche settimane dallo scandalo delle nomine dei membri dell'Autorità per le Garanzie nelle Comunicazioni e di quelli del Garante della privacy, si rendesse protagonista di una nomina tanto importante per il futuro dell'innovazione in Italia ... in totale assenza della trasparenza ....".

Si apprende ora che in sede di conversione del decreto legge n.83, il 23 luglio le Commissioni della Camera VI e X avrebbero approvato alcuni emendamenti,tra l'altro,agli artt.20.21 e 2, cercando di riparare, in qualche modo,agli errori e omissioni del citato DL n.83…Le più significative , riguardanti il presente scritto . sono quelle secondo cui : a) le sole attività amministrative,contrattuali e strumentali. già attribuite a DigitPA, sono trasferite alla Consip che però collaborerà con l'Agenzia nella fase di acquisizione di beni e servizi per l'Amministrazione; b)la composizione del Collegio dei revisori che deve essere composto di tre membri effettivi ed uno supplente ; c) **l'aumento da 30 a 60** giorni del termine entro il quale deve essere adottato il decreto di nomina del direttore generale ,con estensione dei requisiti di qualificazione professionale, già previsti per il direttore generale ,a tutti i componenti del Comitato di indirizzo dell'Agenzia ..Restano ,per il momento,i dubbi sopra citati in ordine al mistero dell'avviso pubblico… Non resta che attendere ,incrociando le dita….