Considerazioni sull'internet degli oggetti e sul *cloud computing*

di *Carlo Sarzana di Sant'Ippolito*

Ringrazio anzitutto gli organizzatori del presente Convegno, e particolarmente la professoressa Ruggeri ed il professor Picotti, per il gradito invito a presiedere la seduta iniziale di questo importante Convegno. Dato il titolo della Sezione, credo sia opportuno accennare ai più recenti sviluppi della tecnologia informatica in relazione ai rischi sociali e giuridici derivanti dall'uso di tali tecnologie, particolarmente per quanto riguarda la sicurezza informatica, la protezione della *privacy* e la tutela dei dati personali.

Ripeto qui per inciso ciò che da tempo vado sostenendo, e cioè che in un settore, quale quello informatico nel quale le nuove tecnologie irrompono, creando necessità, a volte urgenti, di un inquadramento dei nuovi fenomeni nel campo del diritto, è divenuto difficile stare realmente al passo con la situazione giacché occorrono doti di costante attenzione e capacità, di osservazione delle nuove realtà, attenzione e capacità che devono essere accompagnate, ai fini di una comprensione e di un esatto inquadramento del complesso fenomeno, da una sensibilità insieme giuridica, sociologica e criminologica.

Ciò premesso passo ad esaminare, molto succintamente alcuni dei problemi relativi ai rischi sopraccennati. In proposito 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 oggetti, raccogliere dati, trattarli e trasferirli.

Già in occasione della Conferenza Europea sull'argomento "*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 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: per tutelare la sicurezza delle informazioni la Commissione ha chiesto agli Stati di rafforzare la sorveglianza e la protezione delle infrastrutture critiche informatiche [1].

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 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 venduti ai consumatori dovrebbe fornire le necessarie informazioni per determinare eventuali minacce alla stessa vita privata o alla protezione dei dati personali. A questo riguardo la Commissione ha emanato apposite raccomandazioni [2].

---

[1] A proposito dell'IdO un autore francese MARC-OLIVIER PADIS in un articolo dal titolo *Homo numericus – L'Internet e les nouveaut 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 oginariament une réalité dècevant dans de mondes parallèles mais de vivre dans une "réalité augumentée*".

[2] *Applications RFID utilisées dans le commerce de détail*

9. 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'étiquettes placées sur les produits ou incorporées à ceux-ci.

10. Lors de la réalisation de l'évaluation d'impact sur la protection des donne et de la vie privée visée aux points 4 et 5, l'exploitant d'application doit déterminer précisément si les étiquettes placées sur des produits ou incorporées à des produits vendus aux consommateurs par des détaillantes qui ne sont pas exploitants de cette application présentent un risque probable pour la vie privée ou la protection des donne à caractère personnel.

11. Les détaillants doivent désactiver ou retirer, au point de vente, les étiquettes de leur application à moins que les, consommateurs, après avoir pris connnaissance de la politique d'information visée au point 7, acceptent que les étiquettes restent opérationnelles. Par désactivation des etiquettes, on entend tout processus qui interrompt les interactions d'une etiquette avec son environnement et qui n'exige pas de participation active du consommateur. La dèsactivation ou le retrait des etiquettes par le détaillant doivent être effectués sur-le-champ et sans coût pour le consommateur. Les consommateurs doivent pouvoir verifier que la désactivation ou le retrait sont effectifs.

12. 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 détail et restant opérationnelles au-delà du point

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[3], 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/passegger privacy*;
d) *compliance and abuse of state-owned citizen/passegger 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 tecnological advancement*;
l) *non-compliance with date protection legislation.*

Devo ricordare a questo punto per inciso che, già moltissimi anni fa, nei miei primi scritti ed interventi, 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[5]. 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.

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*". Lo stesso legislatore italiano, nell'intento di proteggere alcuni prodotti nazionali, ha introdotto, sembra senza tener alcun conto 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*

---

de vente ne presentment pas de risque probable pour la vie privée ou la protection des données à caractère personnel. Néanmoins, les détaillants doivent metre gratuitement à disposition un moyen aisé de désactiver ou de retirer, immédiatement ou ultérieurement, ces etiquettes.

13. La désactivation ou le retrait des etiquettes ne doit impliquer aucune reduction ni cessation des obligations légales du détaillant ou du fabricant envers le consommateur.

14. Les points 11 et 12 ne s'appliquent qu'aux détaillants qui sont exploitants.

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

[4] Rinvio in proposito alla prima edizione (Milano, 1994) del mio testo dal titolo di allora *Internet e diritto penale*.

[5] Cfr., da ultimo, l'articolo di A. RUSTICHELLI, *Quando l'hacker attacca il pace-maker*, in *Affari e Finanza*, 7 giugno 2010.

concernenti la commercializzazione dei prodotti tessili, delle pelletterie e calzaturieri allo scopo di permettere l'etichettatura dei prodotti *made in Italy* ...[6].

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[7].

Passando ora ad altro argomento rilevo che, come già illustrato in altra sede[8], l'uso delle apparecchiature WiFi non appare sicuro quanto alla protezione delle informazioni e dei dati. Di recente è scoppiato il c.d. caso Google giacché i suoi incaricati, nell'applicazione del servizio *mapping* denominato *Street View*, avrebbero, si sostiene indiscriminatamente, intercettato comunicazioni di sistemi WiFi non protetti, rilevando indirizzi, percorsi, e-mail, passwords, etc. degli utenti. Alcuni Garanti per la protezione dei dati personali di Paesi europei, come la Germania, la Spagna, l'Irlanda e la Svizzera, ma anche l'Italia, hanno aperto un'apposita inchiesta. Secondo un quotidiano italiano (*Il Sole 24 Ore*) Google Italia avrebbe ammesso che le *Google cars* sono in grado di captare le reti *wireless* non protette e gli apparati di reti mobili e di catturare frammenti di comunicazioni elettroniche. Per quanto riguarda l'Italia il Garante per la protezione dei dati personali avrebbe chiesto a *Google* di conoscere la data di inizio della raccolta delle informazioni (di tutte le informazioni, comprese le immagini), e finalità per le quali erano state registrate, la durata e l'indicazione degli archivi erano state conservate. In attesa della risposta della società di *Mountain View* il Garante ha imposto a *Google* di sospendere il trattamento dei dati captati dalle *reti wireless* e dai telefonini, nonché di chiarire se quelle informazioni fossero accessibili a terzi o fossero state cedute; infine, se per catturarle fossero stati utilizzati *software* particolari.

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

Cos'è il 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 in-

---

[6] 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 Ministro 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*".

[7] 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.*

[8] Cfr. il mio testo *Internet, informatica e diritto penale*, Milano, 2010, p. 693 ss.

dubbiamente dei benefici del *cloud computing* in quanto esso consente di ridurre notevolmente i costi associati alle forniture dei servizi: infatti appaiono sempre più numerose le aziende sedotte dalle offerte delle società che forniscono i servizi di *cloud computing*, servizi che vengono ovviamente presentati 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*).

Pa 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*.

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.

Tuttavia vi è il rovescio della medaglia e cioè esistono rischi e pericoli nell'uso e nella gestione del *cloud computing*. Varie organizzazioni hanno esaminato il problema, tra cui la citata l'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 ben 38! In effetti, nonostante le grandi campagne pubblicitarie condotte dalle imprese che commercializzano il sistema, 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 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 di usare il sistema: la percentuale è rimasta fissa rispetto all'anno precedente.

Per quanto riguarda il profilo giuridico del servizio, alcuni pubblicisti italiani hanno cercato di inquadrare il *cloud computing* nel sistema giuridico vigente.

Secondo una prima tesi[9], 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.

Secondo altra tesi[10], sarebbe da escludere la natura di appalto di servizi in quanto si tratterebbe invece di un contratto atipico.

Va detto, a questo punto, che il fenomeno del *cloud computing* ha indubbiamente destato l'interesse del mondo imprenditoriale, apparendo strategico anche per molte grandi aziende come *Google, Amazon, IBM* e per la stessa *Microsoft,* aziende che forniscono la possibilità di creare e gestire documenti di testo, fogli di calcolo e molti altri servizi utilizzando siti Web.

Tuttavia l'organizzazione denominata *Electron Privacy Information Center* ha, di recente, 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 dovute essere tenute sotto chiave sino a quando non l'organizzazione non sarebbe 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 sarebbe stata in grado di dimostrare che le sue pratiche erano adeguate, sicure e rispettose della *privacy*[11].

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.

Di *cloud computing* si parla anche fuori degli Stati Uniti, ad es. in seno all'OCSE. Nell'ottobre scorso (2009) 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.*

Non può non rilevarsi a questo punto che critiche incisive all'uso del *cloud computing* sono state formulate dal noto *hacker* Richard Stallman, fondatore della *Free Software Fondation*, che lo ha definito come una mossa tipicamente pubblicitaria che metterebbe i dati degli utenti su *server* remoti, in balia dei fornitori dei *server* stessi[12].

---

[9] Cfr. S. BENANDI, *Software as a Service (Saas): aspetti giuridici e negoziali*, in *www.stefanobenandi.com/software-as-a-service-aspettigiuridici.*

[10] Cfr. F. NICOLA, *I nuovi paradigma della rete. Distribued computing, cloud computing, computing paradigms: abstract sugli aspetti e profili giuridici*, in *www.diritto.it/art.php?file=/archivio/27973.html* vedi anche R. FREATO-S. COSSINCARE, *SLA in 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 *adde*, H. CARADOU, *Le droit dans les nuages*, in *ivi*, luglio 2010, p. 251; Above the cloud, di autori vari, in *http://berkeleyclouds.blogspot.com* dell'11 giugno 2009; *La révolution du cloud computing*, di P. DESMDT, in *www.usinenouvelle.com/article/la-revolution-du-cloud-computing.*

In materia di rischi derivanti dall'uso del *cloud computing* vedi anche il *paper* dal titolo *The drivers for web security in the cloud* di F. HOWARD del febbraio 2010, cui *adde* INFO-WORD, *Cloud Computing deep dive*, special report del settembre 2009. Vedi anche il *paper* dal titolo *From virtualization vs security to virtualization based security*, dell'ISACA, Intel Corporation del 2007. Infine vedi il *paper* dal titolo *What the ideal cloud-based web security service should provide*, di F. HOWARD, febbraio 2010.

[11] Cfr. MARUCCI, *USA. Cloud computing sul banco degli imputati* in *www punto-informatico.it* del 19 marzo 2009.

[12] R. STALLMAN in un'intervista al *Guardian* ha 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*

Per concludere devo dire che non mi sento di dare torto alle critiche ed ai giudizi 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 elaborato programma di penetrazione, di individuare nel settore privato ma specialmente in quello pubblico, i possibili *decision makers* (tecnici, burocrati e politici) 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, in realtà finalizzati a reclamizzare la bontà dei prodotti ed i vantaggi delle innovazioni proposte. In pratica i problemi, quasi sempre esistenti, relativi principalmente alla sicurezza delle innovazioni ed alla tutela dell'ambiente, vengono disinvoltamente ficcati "sotto il tappeto", ignorati o minimizzati e, 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 la sua adozione nel settore pubblico. Staremo a vedere!

Vi ringrazio per la Vostra attenzione.

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.linuks-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.linuks-magazine.com*, 1° ottobre 2008.