Mercati digitali, innovazione tecnologica, sicurezza informatica: la visione nazionale e internazionale

Spunti problematici per il semestre di presidenza europea[1]

Elisabetta Zuanelli

1. Premessa

La crescita esponenziale dell'innovazione tecnologica nell'ICT e dei mercati digitali connessi interroga sulle modalità dello sviluppo, sulle regole e sulle tematiche inerenti i vantaggi conseguenti e i possibili ostacoli connessi alla qualità dello sviluppo e del mercato digitali e ai potenziali rischi di *cybersecurity* implicati.

Un approccio interdisciplinare ai temi dello sviluppo della ricerca e del mercato nella prospettiva nazionale e nel contesto europeo internazionale, che confronti aspetti tecnologici, giuridici, economici e sociali, consente di intervenire sulla definizione complessiva delle politiche dello sviluppo, sulle risorse disponibili, sulla qualità e la funzionalità dei prodotti e dei servizi ICT prefigurati.

Il semestre di Presidenza italiana dell'Unione europea che si è aperto richiede uno sforzo congiunto di analisi, proposte e intesa tra istituzioni pubbliche e della ricerca, attori piccoli e grandi del mercato e dell'economia digitale, anche in prospettiva occupazionale e profili di costituzione condivisa di un "bene sociale" di nuova generazione rappresentato dalle risorse tecnologiche dell'ICT.

[1] *Paper* presentato al convegno di ugual titolo, Roma, 10 luglio 2014; vd. *Editoriale*.

2. I mercati digitali

Una prima riflessione sulla nozione di *mercati digitali* invita a collocarli nell'ambito dell'economia digitale che tratta di Reti, *hardware* e *software* prodotti con geometrica moltiplicazione nel presente micromillennio. Prodotti e servizi digitali sono l'oggetto sociale di aziende e di enti produttori che configurano l'offerta, in risposta a una domanda implicita o esplicitata di soluzioni innovative nella gestione dell'informazione informatizzata e nella creazione di nuovi prodotti e servizi per scopi diversi, a vantaggio di organizzazioni, istituzioni, aziende e cittadini. Questi consumatori, con specifica attenzione all'interazione in Internet e in Rete, sono la risposta all'offerta.

E-commerce, e-banking, e-government, e-gambling, e-business, piattaforme *social*, motori di ricerca, portali e i più svariati "servizi digitali" nelle "*app* per *mobile*", oltre ai tradizionali sistemi informativi aziendali più o meno intelligenti, sono ambiti di interazione virtuale acceduti con dispositivi fissi e mobili.

Oggi lo sviluppo del mercato dei servizi *mobile* supportato da *smartphone*, iPad e altro segnala un'esplosione imponente dei consumi. Se il mercato statunitense e quello asiatico in rapida ascesa sono i riferimenti economico-finanziari più rilevanti, la prospettiva di un mercato europeo digitale unico rispetto al contesto globale sollecita quesiti in ordine alle opportunità, alle regole, ai vincoli, ai monopoli e alle logiche dello sviluppo sottese.

Di questo cominciava ad occuparsi l'iniziativa di "Europa elettronica" lanciata a Lisbona nel 2000, prospettiva che ha accelerato la consapevolezza del valore competitivo dell'ICT per le economie dei sistemi Paese e del ritardo tecnologico negli stati membri.

E-Europe, *i-Europe* ed Europa 2020: di questo si occupavano e si occupano agende attente allo sviluppo di servizi transfrontalieri nel pubblico e investimenti nel *R&D* dell'ICT europeo. La situazione odierna appare oggi assai problematica.

2.1. Alcuni dati

Il rapporto Assinform 2014 ci informa che l'ICT mondiale nel 2009-2012 è cresciuto a una media del 3,8%; nel Nord America con il +3,5%, in Asia e nel Pacifico del +6,6%, in America latina del +5,8%. Gli investimenti ICT % sul PIL sono stati in Italia del 4,8%, contro una media Ue del 6,5%; in Germania del 6,8%, in Francia del 7%, nel Regno Unito del 9,6%.

Il mercato ICT nel 2013 registra nel mondo un +3,8% mentre l'Europa si ritrae a un -0,9% e l'Italia a un -4,4%. In Italia sono in calo dispositivi e sistemi, mentre mantengono un *trend* positivo *software* e soluzioni ICT. In grande crescita sono i servizi ICT e di Rete e in buona crescita *e-content* e *digital advertising*.

A questi *trend* corrispondono quote di mercato che vedono in testa i giganti Apple, Google, Amazon, Facebook con ambiti relativi ai giochi *online*, all'editoria, ai mercati immobiliari, al turismo, ai media, al web marketing, alla pubblicità digitale, alle tecnologie e ai servizi dell'informazione a rischio (RITS), all'Internet delle cose (sensori, droni, *smart city* e così via).

Rispetto agli andamenti del mercato mondiale, i dati di mercato riscontrabili in Eurostat segnalavano nel recente passato la presenza di vecchi criteri e l'assenza di informazione economica. Il quadro Eurostat del mercato digitale era così presentato:

> the completion of a single European information space innovation and investment in ICT research achieving an inclusive European information society.

Le agende europee al 2011 contenevano temi variabili dal concetto di *green economy* ai servizi digitali alle persone, alle famiglie e alle imprese, dall'identità alla sicurezza digitale in un mix non sempre organico di visione e sviluppo.

Il risultato più recente nell'evoluzione delle priorità da perseguire è rappresentato, come vedremo nell'Agenda 2012, da prospettive articolate e diverse rispetto agli schemi precedenti in ordine agli obiettivi, in particolare del mercato.

2.2. L'economia digitale

La prospettiva di un'economia digitale globale è un tema da sviluppare nelle diverse implicazioni economiche, giuridiche, sociali, istituzionali e occupazionali. Quesiti da affrontare in chiave nazionale e internazionale europea interrogano su:

- come si regolano i singoli stati nazionali;
- come si regolano le economie correlate, europea e internazionale;
- come sono governate le economie digitali: investimenti, gradi di libertà, ritorno economico, garanzie socio-economiche, monopoli;
- quali gli obiettivi delle Agende digitali nazionali ed europee e in quale rapporto.

Un'affermazione fondamentale proveniente da documenti europei propone di trattare le tecnologie ICT come nuovo *bene comune* di interesse generale. Occorre dunque far crescere le nuove competenze economiche, giuridico-normative, tecnologiche, sociali in materia digitale e occorre una nuova visione interdisciplinare, nuove progettualità e nuova occupazione. I "nativi digitali", giovani cresciuti nell'ambiente delle tecnologie virtuali, non sono per ciò i nuovi "competenti", ma solo nuovi consumatori

Il tema *regolazione* si presenta come un mosaico sfaccettato ancora latente: ai vari livelli le regole sono poche e disomogenee; quasi assenti quelle interstatuali. Tematiche giuridico-normative e legali investono la contrattualistica, i monopoli, la protezione dei dati, il diritto d'autore.

La vendita dei prodotti e dei servizi fisici della *old economy* si è enormemente ampliata con la vendita dei prodotti e dei servizi virtuali della *new economy*: nell'economia come nella finanza, nelle banche come nelle assicurazioni, nei prodotti digitalizzati (film, musica, giornali) come nella pubblicità, nei servizi relazionali e/o professionali e nelle *governance* aziendali come nel *government* pubblico.

Insieme all'ampliamento dei prodotti e dei servizi digitali stiamo assistendo allo sviluppo crescente dell'*economia del cybercrime* nelle

sue varie declinazioni: virus, *malware*, *hacking*, furto di dati personali, nonché la gestione *online* di *asset* criminali quali la prostituzione, la pedofilia, la droga, il traffico di denaro sporco. Il mondo virtuale ottimizza anche le peggiori realtà del mondo fisico.

Ciò sollecita interventi di varia natura che riducano i rischi della virtualità e *garantiscano* i consumatori, cittadini, istituzioni, aziende, nella fruizione dei benefici dell'innovazione tecnologica. È, come vedremo oltre, il tema della *sicurezza informatica*, cui ci invitano il Parlamento europeo e l'Unione europea.

2.3. Il mercato unico digitale

L'idea diffusa e propugnata dal Parlamento europeo[2] e dall'Unione europea sui vantaggi di un mercato unico digitale merita attenzione e valutazione specifica in ordine a questi temi:

i. quali prodotti e servizi possono essere ricompresi sotto la nozione di mercato unico;
ii. quali regole per il *procurement* e le gare in materia;
iii. quali prospettive di sussidiarietà rispetto al mercato convenuto a livello europeo.

Mentre il ritardo tecnologico segnalato nel lontano 1994 dal *Libro bianco* di Jacques Delors ha accelerato programmi, agende e consapevolezza, è chiaro che una politica unitaria nel mercato digitale non può che confrontarsi con le singole situazioni nazionali e con le relative agende specifiche.

La riformulazione al 2012 dell'Agenda digitale europea prevedeva questi *item*:

1. la creazione di un ambiente regolatorio nuovo della banda larga;
2. nuove infrastrutture digitali pubbliche attraverso i prestiti della *Connecting Europe Facility*;
3. lancio della grande coalizione sulle abilità e sull'occupazione digitali;
4. proposta di una strategia e di una direttiva Ue sulla *cybersecurity*;

[2] http://www.europarl.europa.eu/aboutparliament/it/displayFtu.html?ftuId= FTU_5.9.4.html

5. aggiornamento del quadro Ue sul *copyright*;
6. accelerazione nel *cloud computing* attraverso il potere d'acquisto del settore pubblico;
7. lancio di una nuova strategia industriale elettronica, *Airbus of Chips* (il raddoppiamento del numero di processori per lo sviluppo dell'IoT, *Internet of things*).

La DAE attuale 2014 (Agenda digitale per l'Europa) contiene tredici obiettivi specifici per il cambiamento che si intende realizzare:

1. tutta l'Ue da coprire con la banda larga entro il 2013;
2. tutta l'Ue da coprire con la banda larga superiore a 30 Mbps entro il 2020;
3. il 50% della media Ue dovrebbe passare alla banda larga sopra i 100 Mbps entro il 2020;
4. il 50% della popolazione dovrebbe acquistare *online* entro il 2015;
5. il 20% della popolazione dovrebbe acquistare nell'*online* transfrontaliero entro il 2015;
6. il 33% delle PMI dovrebbe vendere e acquistare *online* entro il 2015;
7. la differenza tra *roaming* e tariffe nazionali dovrebbe avvicinarsi a zero entro il 2015;
8. aumentare l'uso di Internet regolare dal 60% al 75% entro il 2015, e dal 41% al 60% tra le persone svantaggiate;
9. dimezzare la percentuale di popolazione che non ha mai usato Internet dal 30% al 15% entro il 2015;
10. il 50% dei cittadini dovrebbe utilizzare l'*e-Government* entro il 2015, con oltre la metà di ritorno di moduli compilati (?);
11. tutti i principali servizi pubblici transfrontalieri, concordati da parte degli Stati membri nel 2011, dovrebbero essere disponibili *online* entro il 2015;
12. raddoppiare gli investimenti pubblici nel *R&D* a 11 miliardi di euro entro il 2020;
13. ridurre il consumo energetico di illuminazione del 20% entro il 2020.

La lettura di questo programma evidenzia tre linee di sviluppo incentrate sui consumi e le infrastrutture: potenziamento importante del-

la banda larga, sviluppo consistente dell'*e-commerce*, potenziamento dell'uso della rete mediante tariffe e nuovi servizi, in particolare nel pubblico; attenzione infine alla ricerca e agli investimenti nella stessa.

Traiamo conferma di alcune di queste linee di sviluppo incentrate sui consumi dallo *scoreboard* 2014 riportato in Figura 1 che cita come criteri di misurazione attività digitali che vanno dall'uso della posta elettronica alla ricerca di informazione commerciale e turistica, dalla lettura di giornali all'uso dei *social media*, dall'interazione con le autorità pubbliche all'*internet banking*, dalla vendita all'acquisto *online* di contenuti (film, musica, *software*), di beni e servizi.

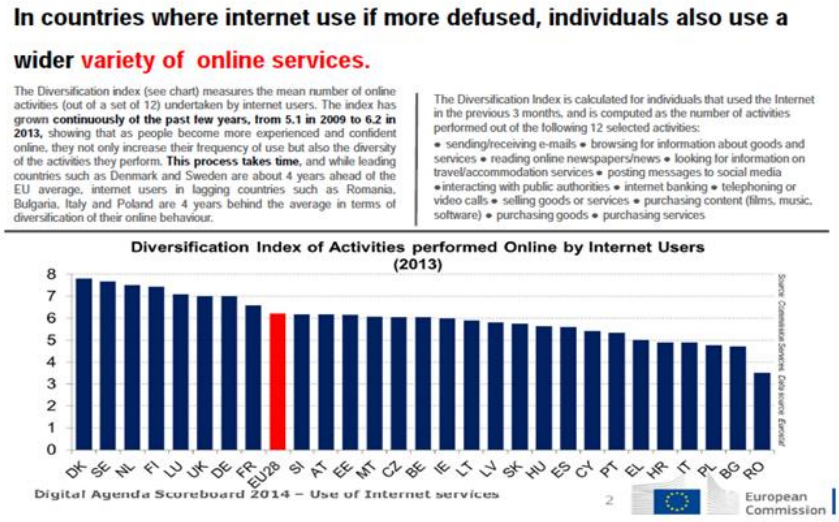

Figura 1. *Digital Agenda Scoreboard* 2014. Uso di servizi Internet (Fonte: Commissione europea)

Ciò che dovremo approfondire, oltre alla domanda, è l'offerta, la capacità di produrre e vendere gli "oggetti" indicati nel mercato digitale da parte di aziende europee e nazionali. Il ritardo o l'assenza di un'imprenditoria locale capace di competizione è senza dubbio uno dei temi del mercato unico digitale.

Insieme va potenziata l'effettiva possibilità di assorbimento di nuova occupazione connessa a nuove professionalità, tema che confronta gradi di acculturazione digitale largamente disomogenea nella Ue. È il

tema enunciato come uno dei dieci obiettivi prioritari dalla nuova presidenza europea: il mercato unico digitale "connesso" che dovrebbe generare una crescita aggiuntiva di 250 miliardi di euro dal 2014 al 2019 e creare "centinaia di migliaia di nuovi posti di lavoro" in una "vibrante società della conoscenza":

> Creating a connected single digital market is one of the ten priorities from the President-elect Jean-Claude Juncker. Its completion could generate up to EUR 250 billion of additional growth in Europe in the course of the mandate of the new Commission (2014-2019), thereby creating hundreds of thousands of new jobs, notably for young job-seekers, and a vibrant knowledge-based society[3].

Queste le parole del nuovo presidente Ue Jean-Claude Juncker:

> I believe that we must make much better use of the great opportunities offered by digital technologies, which know no borders. To do so, we will need to have the courage to break down national silos in telecoms regulation, in copyright and data protection legislation, in the management of radio waves and in the application of competition law[4].

In altri termini, il mercato europeo digitale, in larga misura di importazione per le diverse tipologie di servizi digitali, aumenterà di volume nei consumi e forse nell'occupazione. La sua prospettazione può senza dubbio implementare politiche importanti di servizi transfrontalieri quali la recepita fatturazione elettronica o l'identità digitale. Tutto il resto necessita di una logica di revisione dei mercati, della concorrenza, della crescita dimensionale delle aziende, delle gare e dell'importazione tecnologica stessa. A questo nuovo mercato sono chiamate in prima fila le amministrazioni dello stato e i loro servizi digitali.

La tecnologia di *retrieval* dell'informazione all'interno di imprese e organizzazioni è attualmente nota come *enterprise search engine*. È una declinazione particolare dell'*information retrieval* in un dominio

[3] http://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-recent-trends-use-internet-services-and-applications-eu-2014

[4] http://ec.europa.eu/digital-agenda/en/news/scoreboard-2014-recent-trends-use-internet-services-and-applications-eu-2014

dai contorni e dalle specifiche ben definite e chiaramente determinabili in una micro area di conoscenza rispetto a quella macro del Web. È un ambito in cui l'informazione può essere sia strutturata sia non strutturata; può comprendere un ampio e diversificato numero di fonti, altrettanto di linguaggi, formati e diritti di accesso ai dati che differiscono tra gli impiegati.

3. L'Amministrazione digitale e l'innovazione tecnologica

In un mio contributo recente ho cercato di inquadrare il difficile tema, alla luce di nozioni quali quelle di comunicazione organizzativa e servizi digitali, intesi come visione d'insieme della nuova produttività amministrativa, tanto nella prospettiva nazionale quanto in quella europea[5].

Per il nostro Paese ho segnalato alcuni temi chiave per un reale efficientamento del sistema. L'indecidibile qualità della spesa informatica in Italia, registrata nei passati governi, sconta infatti una serie di problemi di visione, di obiettivi funzionali e di controllo dell'allocazione delle risorse, nell'ambito dell'amministrazione pubblica centrale e locale. Le ragioni sono molteplici. Nell'ordine si possono citare:

a) *l'ignoranza di sistema e la delega totale all'offerta di mercato* ICT. L'offerta di mercato, come è facile constatare, non è stata e non è in grado da sola di offrire soluzioni e servizi digitali coincidenti con le necessità gestionali amministrative. Un procedimento o un servizio amministrativo non si sviluppa automaticamente appoggiandolo a una piattaforma informatica esterna, per avanzata che sia. Soluzioni di tipo *cloud*, logiche partecipative e di apertura dei dati pubblici appaiono oggi in parte azzardate e in controtendenza rispetto alle esperienze internazionali. ENISA, ente dell'Unione europea che si occupa delle reti e della sicurezza dell'informazione *online*, ha messo

[5] E. ZUANELLI, *Amministrazione digitale e innovazione tecnologica*, Aracne, Roma, 2013

ripetutamente in guardia sui rischi che l'esternalizzazione e la fruizione a distanza dei dati comporta, con i tre più recenti rapporti: ENISA 2009, 2011 e 2012. Gli Stati Uniti hanno avviato un piano potente di gestione della sicurezza dell'informazione e di eventuali progetti *cloud* attraverso le Agenzie federali, un robusto *board* centrale e un apposito programma centralizzato e decentrato. Oggi contiamo sul Piano nazionale sulla sicurezza e sulle convergenze europee in materia di regolazione, visione da precisare per una valutazione effettiva sui ritorni economici degli investimenti in *data centre* aggregati*;*

b) *l'eventuale risparmio di spesa nelle soluzioni* cloud *dovrebbe essere verificato con cauti progetti sperimentali e con soluzioni particolari, a livello locale, che non investano l'uso di dati* core *e sensibili, come suggerisce l'Ue.* In ogni caso, il risparmio immaginato non coincide con l'efficienza nella gestione dei procedimenti amministrativi e dovrà tener conto non solo della sicurezza, ma anche dei costi di migrazione delle basi di dati e dello sviluppo di procedimenti e servizi amministrativi a supporto digitale, nella prospettiva di una diversa efficienza operativa delle amministrazioni. Si aggiunga poi la considerazione che la prospettiva di *data centre* di "gestione integrata" di anagrafi, per esempio, pone problemi noti di omologazione delle classificazioni e di conflittualità tra i soggetti detentori di dati.

c) Di contro, *il costo dell'ignoranza informatica delle amministrazioni locali e centrali***,** su cui ha riferito nel recente passato l'Università Bocconi, si riscontra agevolmente, confrontando il disordine concettuale *storico* dei capitoli di spesa e l'impossibilità di un confronto di produttività degli investimenti informatici tra i dati, per amministrazione e capitoli.

d) Fattore delicato in assoluto è poi *la qualità degli investimenti e la congruità dei medesimi***,** che andrebbe valutata su obiettivi

gestionali amministrativi specifici [che cosa significa spendere per "opere dell'ingegno (*sic*!) e *software* prodotto" e per "consulenza informatica"? che cosa rientra nella spesa ICT? come si giustificano le allocazioni di risorse nelle *in-house*? in che cosa consiste la spesa per investimenti?] Il quesito alla base è il ritorno sugli investimenti ovvero il ROI nella gestione dell'informazione e dei procedimenti amministrativi in chiave digitale.

e) Fattore critico ulteriore è l'incapacità d'uso nelle amministrazioni dello stato di *metriche corrette per valutare l'offerta e il benchmarking* nel mercato digitale.

f) Si aggiunga, infine, la spesso lamentata *povertà tecnica dei bandi di gara e un mercato digitale ancora chiuso***,** se non per pochi fornitori selezionati. È auspicabile che quanto previsto dalle nuove prospettive in materia liberalizzi l'offerta e apra il mercato in chiave competitiva per le piccole imprese e le *start-up*, anche in ambito europeo. Resta la responsabilità degli addetti nelle amministrazioni e in particolare della dirigenza pubblica ovvero dei responsabili della domanda e dei bandi di gara o delle assegnazioni.

La situazione rilevata sommariamente nel 2012 spiega il fondo della classifica del nostro Paese in termini di innovazione digitale a livello europeo, salvata dal numero di cellulari e *iPad* per persona che è tra i più alti e dall'attività svolta nell'*e-procurement*.

Vanno affrontate, dunque, con una strategia di sistema, la spesa e la partecipazione all'economia digitale del nostro Paese nella prospettiva locale e internazionale, come capacità produttiva di innovazione digitale di prodotti e servizi. L'innovazione non può essere limitata alle tendenze di moda, ma chiede forme di intervento, orientamento e controllo forti e generalizzate e una strategia economica capace di essere protagonista anche ai tavoli europei.

Si possono avanzare diverse ipotesi immediate, a basso costo e a forte impatto di sistema, da negoziare con gli *stakeholder* del mercato, nella prospettiva di un rilancio serio, difficile ma perseguibile, della

nostra capacità propositiva sulla base di nuove regole, nazionali ed europee. L'economia digitale è una dimensione globale e trasversale totalizzante e fondamentale, nel pubblico come nel privato, per l'economia dei sistemi paese, che richiede, appunto, interventi di sistema, difficili ma necessari.

4. La sicurezza digitale

Affrontare i temi della sicurezza informatica, della protezione dei dati e della *privacy* è approccio complesso e multidisciplinare. Da prospettiva multidisciplinare, è utile richiamare brevemente il dibattito e le informazioni crescenti offerti negli anni dall'Agenzia europea ENISA, da specifiche fonti italiane quali AgCom, il Garante della privacy, AgID e svariate fonti istituzionali e di ricerca europee e internazionali.

Rapporti recenti come la Relazione 2012 di Deloitte e Touch sui principali rischi in ambito di sicurezza includono questi temi[6].

RISCHI

- *Social networking*: protezione del marchio, accesso non autorizzato a dati confidenziali, violazioni regolatorie o legali.
- *Dispositivi mobili*: perdita o rilascio di dati inerenti il *business*, gestione della sicurezza e dell'identità, integrazione nell'ERP.
- *Malware*: perdita o furto di informazione critica, impatti sull'*hardware*, impatto sul *cash*, perdita di produttività.
- *Computing dell'utente finale*: falsa rappresentazione finanziaria, problemi di regolazione, perdita o corruzione dei dati.
- *Spionaggio aziendale*: perdita o rilascio di dati aziendali, negazione del servizio, perdita della proprietà intellettuale.
- *Project Backlog*: ritardi o fallimento di progetto, mancanza di

[6] T. MIZOGOUCHI, *Information Technology risks in today's environment*. Deloitte and Touch, 2012. https://chapters.theiia.org/.../SD_IIA___ISACA_Ev...

controllo e sicurezza su progetti completati, mancato raggiungimento degli obiettivi di *business*, gestione di vendita inadeguata.

- *IT Governance*: incapacità di gestione dei controlli e delle politiche aziendali, impatti operativi, rischi nella sicurezza dell'informazione, violazioni regolatorie, duplicazione di impegno, aumento dei costi, inefficienze.
- *Electronic Records Management* (ERM): perdita dei dati nei processi di conversione, violazioni regolatorie se non esistono controlli adeguati, questioni forensi, *storage* e mantenimento.
- *Gestione dei dati*: penalizzazioni regolatorie, danno d'immagine, aumento dei costi di *compliance.*
- *Cloud Computing*: accesso amministrativo, gestione dei dati-localizzazione, *compliance*, recupero, sicurezza, problemi di connessione internet e del fornitore *cloud*, supporto investigativo, viabilità a lungo termine.

Questo crudo elenco 2012, accompagnato da indicazioni operative per la gestione dei rischi, non può essere considerato una rappresentazione allarmistica, ma una visione complessiva degli ambiti di intervento in chiave tecnologica e organizzativa che merita attente valutazioni e strategie di sistema.

D'altro canto, in uno studio sui rischi e sui vantaggi dell'adozione di tecnologie *cloud* il Rapporto ENISA 2009 concludeva che:

> The cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective.

Il Rapporto ENISA 2009 poneva all'attenzione degli *stakeholder* internazionali europei rischi di sicurezza nell'adozione del *cloud* quali:

- la perdita di *governance*;
- il *lock-in* ovvero la portabilità dei dati;
- il fallimento dell'isolamento di *storage*, memoria, *routing*;
- rischi da *compliance* del *cloud provider* per regolamentazione carente o inesistente o locale;

- il compromesso delle interfacce di gestione;
- la protezione dei dati (controllo e legalità);
- la cancellazione dei dati non sicura e incompleta;
- gli *insider* maligni: usi illeciti.

Sui temi della sicurezza e della privatezza fonti diverse menzionano, a titolo d'esempio, cinque aspetti principali:

- *la gestione dell'identità per l'accesso all'informazione*. Questa può essere lasciata al fornitore, all'interno della piattaforma, o al cliente che la gestisce come crede;
- *la sicurezza fisica della macchina e del personale*. Il fornitore garantisce che le macchine sono adeguatamente sicure e che l'accesso ai dati è non solo limitato ma anche documentato;
- *la disponibilità del servizio*. Il fornitore assicura i clienti che avranno accesso regolare ai loro dati e alle loro applicazioni;
- *la sicurezza delle applicazioni*. I fornitori garantiscono attraverso test e procedure specifiche le applicazioni esterne;
- *la privacy*. I fornitori garantiscono non solo il mascheramento dei dati e l'accesso ai soli utenti autorizzati, ma anche la protezione delle identità e delle credenziali digitali.

Nel Rapporto ENISA 2011 si affermava che:

> Governments are recommended to adopt a staged approach in integrating cloud computing into their operations because the complexity of the cloud environment that introduces a number of unknown variables for which Public administrators (PAs) will need to build new approaches to assessing and managing risks.

Dunque, cautela nel pubblico per il numero di variabili sconosciute e necessità di nuovi approcci nella definizione e nella valutazione dei rischi.

In ENISA 2012 ancora:

> The national authorities should take the lead in enhancing the efficiency and effectiveness of information sharing and security

> notification schemes. They should adapt collected and disseminated information to the needs of participating organisations while maintaining statistics about all kinds of information collected. They should establish feedback loops with all types of stakeholders concerned and they should ensure that the economic perspective is duly taken into account when establishing the SNS. Finally, they should assess barriers and benefits of security notification schemes on an ongoing basis.

In buona sostanza, necessità di una disseminazione dell'informazione tra i diversi *stakeholder* e definizione delle barriere e dei benefici derivanti dalle notifiche di sicurezza. A queste indicazioni e sollecitazioni sta rispondendo la strategia nazionale. Nella presentazione del Piano per la sicurezza informatica 2013 l'Agenzia per l'Italia Digitale proponeva le seguenti azioni:

> L'Agenzia è chiamata a dettare raccomandazioni, strategie, norme tecniche in tema di:
> 1. sensibilizzazione e alfabetizzazione del personale in materia di sicurezza informatica e di relative emergenze;
> 2. metodologia di rilevazione ed analisi dei rischi connessi all'impiego di tecnologie evolute;
> 3. valutazione dell'impatto – nel quadro della riservatezza e della sicurezza – dell'avvio di iniziative di automazione;
> 4. esame e stima delle misure di protezione poste in essere e delle eventuali attività di misurazione delle prestazioni.
> L'Agenzia d'intesa e con la partecipazione delle amministrazioni interessate, provvede inoltre a:
> 1. promuovere progetti coerenti con gli obiettivi di cui sopra;
> 2. accertare periodicamente il livello di sicurezza e riservatezza dei sistemi informatici e delle reti telematiche geografiche e locali utilizzate dalle amministrazioni stesse;
> 3. proporre interventi correttivi e suggerire rimedi alle eventuali carenze tecniche, procedurali e organizzative rilevate in sede di riscontro periodico.
> L'Agenzia è impegnata ad avviare, gestire ed evolvere il CERT della PA, in un quadro di coordinamento strategico con altri CERT e di creare una community preparata, aggiornata e che condivida politiche ed azioni in materia di Cybercrime e di coordinamento delle politiche di sicurezza informatica in tale settore.

E, ancora:

NECESSITÀ OPERATIVE

- definire scenari di valutazione del rischio, coinvolgendo le strutture adeguate;
- definire piani di difesa;
- attivare strumenti tecnici ed organizzativi su tutta la filiera;
- coordinare le azioni con «alleati» esterni;
- monitorare e aggiornare costantemente procedure, prassi e strumenti;
- sensibilizzare sulla necessità di *skill* e strumenti multidisciplinari;
- attivare piani di informazione e formazione

L'acquisizione e la gestione di conoscenza quale strumento strategico e operativo, non solo informativo, è alla base della grande rivoluzione informatico-telematica del terzo millennio. Il potere dell'informazione gestita è un valore economico e sociale sul quale si confrontano oggi le economie dei sistemi Paese.

Sul tema della sicurezza informatica, dunque, l'azione del Parlamento Europeo, dell'Ue e di piattaforme come il NIS/ENISA sta avviando in ambito internazionale progetti incentivanti soluzioni tecnologiche preventive del rischio che richiedono forti interventi nello R&D di sistema, inclusa la sensibilizzazione della più vasta platea dei soggetti implicati, in particolare nell'educazione a comportamenti consapevoli in ambito gestionale e organizzativo. Le tecnologie da sole non bastano.

L'ENISA suggerisce approcci interdisciplinari tra i vari *stakeholder* e l'avvio di una metrica per la valutazione dell'impatto economico degli investimenti in materia, il ROSI.

La percezione e la valutazione della sicurezza a favore dei vantaggi offerti dalle nuove tecnologie è un dato strutturalmente rilevante che non deve scoraggiare l'adozione di tecnologie innovative quali quelle *cloud*, ma accompagnarsi a una crescente consapevolezza dei rischi per la sicurezza digitale negli enti, nelle aziende e nelle istituzioni pubbliche e private.

La conoscenza delle tecnologie informatiche disponibili e le norme insufficienti in materia di protezione dei dati si scontrano infatti con livelli crescenti di *cybercrime* e attacchi sempre più virulenti, come

dimostrano i dati citati dai rapporti Clusit, acquisiti da AgID per avviare il monitoraggio e la strategia di sistema. Innovazione tecnologica e rischi di sicurezza dell'informazione sono fenomeni paralleli che continueranno a procedere in parallelo nel futuro e che dovranno competere per garantire i nuovi mercati.

In questa prospettiva, l'attivazione di OSI, Osservatorio sulla sicurezza informatica, avviato dal GAT della Guardia di Finanza insieme al CReSEC dell'Università di Roma "Tor Vergata", al CNR, e ad aziende qualificate è un approccio di servizio alle attività istituzionali. L'obiettivo è di interesse generale e non esclusivo nella prospettiva di una condivisione di sistema, a supporto di scelte e di decisioni in materia.

5. Il Progetto OSI

Nell'interesse istituzionale motivato da AgID e dall'Unione europea per un tema irrinunciabile dello sviluppo economico quale l'economia digitale, l'Osservatorio sulla sicurezza informatica OSI si propone di predisporre strumenti conoscitivi e operativi della sicurezza. In questa logica, come detto, le dotazioni nazionali vanno messe a fattor comune creando una *community* di soggetti compartecipi.

Il Progetto OSI, avviato con una *steering committee* istituzionale pubblica e privata, si va articolando in quattro sottogruppi: economico, giuridico, tecnologico, sociologico-comunicativo.

Sul *piano economico*, a titolo esemplificativo, occorrono analisi e metriche per analizzare e stimare l'impatto della sicurezza e i tipi di sicurezza implicati, sulla base di valutazioni diverse per *stakeholder*:

- dati personali;
- piccole e medie imprese;
- grandi imprese;
- istituzioni.

Serve altresì stimare i *vantaggi economici* offerti da forme di elaborazione più efficienti, da consumi *on demand* e da specifici investimenti in sicurezza (ROSI).

Sul *piano giuridico*, tematiche quali la protezione, la privatezza e la riservatezza dei dati nella legislazione nazionale, europea e interna-

zionale, aspetti contrattuali e negoziali, metriche di valutazione contrattuale SLAs e QoS sono di rilevanza prioritaria e sollecitano confronti internazionali, europei e locali e proposte utili anche in chiave di normazione ascendente europea.

Sul *piano tecnologico* e della resa dei servizi, i livelli di qualità e le prospettive di difesa da attacchi cibernetici e da usi irrituali devono corrispondere a soluzioni innovative della ricerca in materia, l'acquisizione e il testaggio delle soluzioni tecnologiche disponibili, la diffusione presso gli operatori/clienti della conoscenza delle tecniche e delle tecnologie della sicurezza e delle buone pratiche e così via.

Sul *piano sociologico comunicativo*, vanno valutate *la percezione e la conoscenza delle tecnologie e dei rischi della sicurezza* nella triplice prospettiva dei vantaggi del mercato, delle aziende, delle istituzioni e del cittadino.

A titolo di primo contributo conoscitivo, CReSEC/Università di Roma "Tor Vergata" ha messo a disposizione il sito informativo partecipativo già attivo www.cresec.com/cloud e www.cresec.com/tecnologie e propone di assemblare, riorganizzandole in chiave satellitare, le informazioni e le basi di dati già disponibili in siti diversi. Una goccia in un mare complesso di competenze e iniziative che devono essere concrete, non estemporanee, permanenti.