

## 4. Mercati e tendenze

### 4.4 La sicurezza e l'ICT

di Federica Silvestrini\*

**ESTRATTO.** *Quando si parla delle tecnologie dell'informazione, tutti dimostrano grande sensibilità e attenzione ai problemi di sicurezza. La domanda è: ma quei problemi sono veri e reali solo in presenza dell'ICT? E la sicurezza attraverso la tecnologia è sempre indispensabile?*

Con le pubblicazioni del “Codice della privacy”<sup>1</sup> e del “Codice della Pubblica Amministrazione Digitale”<sup>2</sup> (noto come Codice PAD) sono stati affrontati sotto aspetti diversi problemi legati alla sicurezza sia fisica sia logica e normate alcune operazioni di gestione procedurale – come il protocollo, la posta e così via – attraverso il loro collegamento ad alcune tecnologie che dovrebbero essere di ausilio per garantire o risolvere le tematiche connesse. La firma digitale viene unita in maniera indissolubile alla posta che diventa “certificata”, la *smart card*<sup>3</sup> alla Carta d'Identità Elettronica o alla Tessera Sanitaria e altro ancora.

La grande e forse eccessiva attenzione alle tecnologie dell'informazione e della comunicazione solo in funzione di “garanzie” di sicurezza per la loro adozione cominciano a suscitare più di una perplessità e più di due obiezioni. Forse sarebbe utile partire, come spesso sostiene un caro amico, “dai razionali primi”. Si consideri una qualsiasi procedura tradizionale, legata alle norme e alla prassi.

Primo razionale: come viene gestita la procedura per via cartacea.

Ognuno ha ben presente la propria realtà lavorativa e non; nella vita di un'azienda normale, che è la maggioranza dei casi, facilmente assocerà alle persone dell'Ufficio alcune pile di carta sulle scrivanie, faldoni visibili negli schedari facilmente accessibili ai propri collaboratori, archivi di accesso controllato, ma non improbo.



**Figura 1.** Il web manuale.

<sup>1</sup> D. Lgs. 30 giugno 2003, n. 196.

<sup>2</sup> D. Lgs. 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale”, in *GU* n. 112 del 16 maggio 2005 - (Suppl. Ordinario n. 93), modificato con il D. Lgs. 4 aprile 2006, n. 159, in *GU* n. 99 del 29 aprile 2006.

<sup>3</sup> *Smart card*: “è una carta di identificazione, normalmente usata per l'*autenticazione forte* di coloro che la possiedono. Si compone di un supporto plastico, di dimensioni e fattura normalmente identiche a quelle delle carte di credito e di un microprocessore che contiene dati sia protetti che di libero accesso.” Definizione estratta da: <[http://it.wikipedia.org/wiki/Smart\\_card](http://it.wikipedia.org/wiki/Smart_card)>.

Serrature di sicurezza, accessi blindati, cassaforti documentali fanno parte della cultura di poche aziende rispetto alla totalità, aziende che trattano materie e prodotti particolari. La norma è *facilità e semplicità* all'interno dell'organizzazione e dell'ambiente lavorativo, nel rispetto delle leggi comunque.

Secondo razionale: quali sono le misure di sicurezza garantite per salvaguardare i documenti, soprattutto i dati contenuti e trattati. In funzione delle norme e delle proprie competenze, a meno che non siano trattati dati sensibili, le accortezze sono quelle connesse alla normale gestione dei documenti: cartelle, faldoni, armadi e scaffalerei e così via. comunque accessibili al personale competente.

Quando la stessa procedura viene pensata, immaginata ed eseguita con l'ausilio delle tecnologie, improvvisamente ci si ricorda della sicurezza e si pretendono dallo strumento delle garanzie che nessuno si ricorda o immagina di pretendere dall'analogo “manual-cartaceo”.

In sintesi, la percezione generale in tema di sicurezza è che chiunque si ritenga in dovere di sopporre pericolose le tecnologie ICT a priori e di richiedere alle stesse quelle garanzie per la sicurezza che lo strumento in quanto tale non potrà mai dare. Allo strumento vengono poi associati dei concetti amministrativi, già poco chiari a livello cartaceo, creando dei “mostri digitali”: il “documento informatico”, che è tale solo se correlato strettamente alla firma digitale; la posta elettronica, certificata anch'essa tale solo se firmata digitalmente; la Carta Nazionale dei Servizi e così via.



**Figura 2.** Un modo originale di interpretare la sicurezza.

Perchè definirli “mostri digitali”?

Per chi ha seguito le accese discussioni che si sono aperte soprattutto sul Web, non molto seguite con la stessa attenzione dalla stampa tradizionale, i dubbi interpretativi, le incoerenze normative rilevate e le eccezioni sollevate, molto spesso con particolare riguardo alle libertà individuali che ne vengono a soffrire, si possono racchiudere in un'unica, al massimo due, domande: ma tutto questo uso complicato della tecnologia, dovuto alle ineludibili esigenze di sicurezza, a che serve? E se proprio serve, con quale vantaggio o profitto per chi?

Si prenda ad esempio la carta sanitaria su *smart card*; ormai l'hanno ricevuta tutti gli Italiani. Spesso il commento del semplice cittadino è: a che cosa mi serve? il codice fiscale è rimasto lo stesso, allora perchè mi hanno mandato una nuova tessera?

Oppure prendiamo quella cosa degna dei contorcimenti del gruppo del Laocoonte, che è stata descritta sotto la definizione di “posta elettronica certificata”<sup>4</sup>. Tralasciando la confusione mentale generata dalle definizioni di *busta di trasporto* e *messaggio di posta certificata* – entrambe definite “documento informatico” – il solo dato saliente che emerge è che per poterla utilizzare si deve avere la firma elettronica qualificata, la quale non può che essere alla fine di tutti i giri, l'ennesima *smart card*, ovviamente contenente la firma digitale utile a sottoscrivere il documento e la sola a garantire la *sicurezza*. Ma la sicurezza di che cosa, ci si domanda. Vista l'esperienza più che ventennale dei bancomat, penso sia chiaro a tutti che la sicurezza non è relata né identificata con il suo supporto tecnologico, la carta più o meno *intelligente*, ma al fatto che non la si perda o altro.

Allora, perchè creare il mostro digitale istituendo con procedimenti complessi e aggrovigliati una nuova specie di burocrazia, la *burocrazia informatica*, anch'essa lenta e costosa, ma “tanto sicura”. In che cosa consisterebbe, in queste condizioni, lo svecchiamento, lo snellimento, l'economicità dovuti alla introduzione degli *strumenti dell'ICT*? Sono **strumenti** e come tali il loro utilizzo corretto dipende dalle teste o, meglio, dai cervelli pensanti che li utilizzano o insegnano a utilizzarli. L'esperienza dimostra che le tecnologie male utilizzate – non solo quelle ICT – aumentano i costi e alcune volte non solo rallentano i processi, ma ottengono anche risultati imprevisi e del tutto contrari alle attese.

E allora tutta questa esasperazione e attenzione alla sicurezza che gli strumenti ICT debbono garantire sembra quasi l'occasione per la sponsorizzazione di costosi *gadget* che ci fanno dire “io ce l'ho”, ma poco importa a che cosa serve. Il problema resta: “ma quanto mi costi?”



**Figura 3.** "Sarò sicuro?"

### ***Per saperne di più:***

Documentazione e critiche alla firma digitale sono consultabili all'indirizzo  
<<http://www.interlex.it/docdigit/indice.htm>>

<sup>4</sup> D.P.R. 11 febbraio 2005, n. 68.

Documentazione e critiche, dal punto di vista della sicurezza, del Codice della PA Digitale sono consultabili al sito <<http://sicurezza.swzone.it/>>

*\* Dirigente del Ministero Economia e Finanze – Dipartimento per le politiche fiscali.*