

## Privacy! Aiuto o ostacolo per la security?

*Gaetano Rasi, nato a Rovigo nel 1927. Vice presidente della "Fondazione Ugo Spirito" per gli studi filosofici e economici. Già eletto deputato nella XIII legislatura, è stato vice-presidente della X Commissione "Attività produttive" della Camera dal 1996 al 2001.*



*Autore di numerose pubblicazioni, ha diretto la redazione dei 26 volumi degli Annali dell'Economia Italiana, dall'Unità ai nostri giorni (IPSOA, 1982-84).*

*E' stato docente di politica economica nell'Università statale del Molise dal 1987 al 1991 e di economia dello sviluppo e di sociologia economica nell'università di Salerno dal 1991 al 1994. Consigliere dell'Agenzia per il Mezzogiorno (1986-1992),*

*Consigliere di amministrazione della Telecom Italia Spa dal 1994 al 1997, è stato vicepresidente dal 1999 al 2001 del Gruppo Parlamentare italiano per lo Spazio.*

*Nominato nel 1995, Ministro per il Commercio Estero e le Politiche Comunitarie, dal presidente Dini, ha rinunciato all'incarico.*

### Sicurezza e Riservatezza

L'entrata in vigore della normativa sulla protezione dei dati personali ha portato, in tutti i Paesi in cui è stata adottata, sicuri benefici in termini di civiltà grazie al riconoscimento di diritti fondamentali che caratterizzano le società democratiche, ma ha anche fatto sorgere una serie di interrogativi.

Tra i vari interrogativi (la privacy è un ostacolo per il mercato? un costo burocratico? un turbamento per la ricerca scientifica o un ostacolo per gli studi storici? è un freno allo sviluppo? limita le relazioni sociali? intralcia la libertà d'informazione?) uno ha acquisito particolare rilievo nell'ultimo anno: la privacy diminuisce la sicurezza?

Partendo proprio da quest'ultimo interrogativo voglio dimostrare che i timori emersi sono infondati e che anzi la sicurezza richiede una maggiore, e non una minore, tutela dei dati personali.

È evidente che la mancata protezione di grandi banche dati, pubbliche o private, con appropriate misure di sicurezza, comporta il pericolo di violazioni che metterebbero a disposizione di criminali o terroristi informazioni di grande valore. Basti pensare a informazioni di carattere economico, commerciale, sanitario o di difesa o anche a quelle banche dati per le quali, ad uno sguardo superficiale, non si riscontrerebbero pericoli per la privacy come ad esempio nel caso delle liste dei passeggeri delle linee aeree che, contenendo anche preferenze sui cibi, potrebbero rilevare l'appartenenza religiosa di alcuni viaggiatori con la conseguenza di rischi per attentati al volo. La riservatezza al riguardo coincide con la sicurezza. Per brevità non cito altri casi.

Anche mercato e privacy non sono valori necessariamente in conflitto.

Basti pensare che il bisogno di riservatezza e sicurezza dei dati continua ad essere la preoccupazione primaria dei consumatori al punto che lo sviluppo del commercio elettronico passa proprio per la fiducia dei potenziali clienti sul corretto uso che viene fatto dei propri dati e sulle misure di sicurezza adottate a protezione degli stessi dati.

Vi è al riguardo anche un altro aspetto: la sicurezza coincide con la certezza circa l'identità dei soggetti. E questo aspetto è essenziale per il commercio che si svolge tramite reti di Telecomunicazione.

Oramai sono molti i soggetti che si rendono conto dell'importanza di delineare un nucleo essenziale di misure da osservare per garantire la sicurezza dei dati e il rispetto dei principi di correttezza e di pertinenza delle informazioni trattate, sviluppando in tal modo idonee politiche di privacy per presentare ai propri clienti un valore aggiunto.

Questi soggetti sono consapevoli che la concorrenza tra imprese tiene oggi conto di vari aspetti tra cui la qualità del servizio. Qualità che è data anche dal grado di protezione dei dati che una data impresa può offrire e che la rende più o meno competitiva nel mercato.

È evidente, infine, che in questo nuovo scenario la mancanza di tutela della sicurezza dei dati personali può progressivamente diventare un fattore limitante dello stesso sviluppo delle nuove tecnologie o, o per lo meno quantomeno, del loro utilizzo.

Ecco perché io sono convinto che la privacy non debba essere vista come "costo" ma come "risorsa". Ed è questo il tema del convegno internazionale che stiamo organizzando a Roma per il 5 e 6 dicembre prossimi sul rapporto tra la legislazione sulla tutela dei dati personali e l'attività economica; in particolare sull'incidenza delle nuove consapevolezza e del nuovo diritto della persona sui costi e sui prezzi della produzione, dalla fase promozionale a quella post-vendita.

Ma come debbono muoversi i soggetti pubblici e privati in termini di sicurezza?

Innanzitutto è necessaria la conoscenza e la valutazione dei rischi potenziali, la capacità di reazione agli incidenti relativi alla sicurezza, l'aggiornamento costante dei sistemi di sicurezza e, non ultimo, il rispetto dei legittimi interessi dei terzi (siano essi clienti che cittadini).

La proliferazione a livello mondiale dei sistemi informativi e delle reti ha comportato anche il sorgere di nuovi e crescenti rischi che bisogna conoscere per saper affrontare.

I dati e le informazioni conservati e trasmessi attraverso i sistemi informativi e le reti sono esposti a rischi legati a varie modalità di accesso e utilizzazione indebita, alla loro sottrazione o alterazione, alla trasmissione impropria di codici, ad attacchi che ne possono causare la loro distruzione.

La stessa natura e la tipologia delle tecnologie utilizzate sono oggetto di continue modifiche dettate dal progresso.

Ora infatti sono innumerevoli le modalità di accesso alla rete, non solo dispositivi fissi, ma anche sistemi mobili o wireless mentre sono aumentati in misura sostanziale la natura, il volume e la delicatezza delle informazioni trasmesse.

Come è noto la sicurezza non è un concetto statico ma dinamico e pertanto è sempre presente l'esigenza di rivedere le politiche, le prassi, le misure e le procedure correnti. Le procedure da rivedere non riguardano solo le procedure informatiche ma anche quelle a carattere fisico ed organizzativo perché è evidente che la sicurezza riguarda anche il trattamento non automatizzato dei dati (archivi cartacei, trattamenti manuali, ecc.).

È così divenuto indispensabile verificare periodicamente le proprie politiche di privacy valutando regolarmente la loro adeguatezza tramite un'attenta analisi dei rischi. Questa consente di evidenziare le vulnerabilità non solo relative alle componenti tecnologiche, ma anche ai fattori fisici, umani e di carattere organizzativo.

Soluzioni che devono essere proporzionate al valore e alla delicatezza delle informazioni presenti sui sistemi e sulle reti del singolo organismo.

Compito primario del Garante è quello di promuovere una cultura della sicurezza per far comprendere l'importanza di procedere alla pianificazione e alla gestione della sicurezza.

Nello svolgere tale attività il Garante è consapevole che i problemi attinenti la sicurezza devono essere oggetto di attenzione non solo da parte di una ristretta cerchia di addetti ai lavori ma a tutti i livelli governativi della Pubblica Amministrazione e imprenditoriali e in tutti settori sociali. Al riguardo basti pensare ai settori della sanità, a quello bancario e a quello fiscale.

La sensibilizzazione del pubblico, e in particolare degli operatori, rispetto ai rischi ed alle possibili protezioni costituisce la prima linea di difesa per la sicurezza. Conoscere i rischi cui incorrono i sistemi informativi e le reti ed adottare le necessarie politiche e misure per fare fronte a tali rischi, promuovere la formazione e l'aggiornamento di coloro che trattano i dati è la filosofia cui si è ispirata la normativa sulla protezione dei dati personali in materia di misure di sicurezza.

Appare utile sottolineare che lo scorso 25 luglio sono state emanate dall'O.C.S.E. le nuove linee-guida per la sicurezza che si intitolano "Linee-guida per la sicurezza dei sistemi informativi e delle reti: verso una cultura della sicurezza", (nel sito del garante [www.garanteprivacy.it](http://www.garanteprivacy.it) è riportato il testo integrale), linee guida che hanno natura volontaria e sono dirette a governi, imprese e singoli utenti e che appaiono ispirate ai medesimi principi su cui si muove, nell'ambito della normativa sulla privacy, la disciplina della sicurezza.

La legge italiana attualmente definisce e regola le "misure minime di sicurezza"

indicate nel d.P.R. 28 luglio 1999, n. 318 prevedendo per la mancata osservanza sanzioni di carattere penale e civile. Queste regole sono soggette ad adeguamento, con cadenza "almeno biennale", proprio in relazione all'evoluzione tecnica e all'esperienza maturata e pertanto avremo molto presto delle modifiche al regolamento che saranno, probabilmente, contenute nel testo unico sulla protezione dei dati personali previsto per fine 2002.

L'aggiornamento biennale del regolamento permetterà di raccogliere le indicazioni che sono emerse dalla prima esperienza di applicazione della normativa e di tenere conto dei grandi mutamenti intercorsi nel frattempo.

L'adozione del regolamento operata con l'emanazione del d.P.R. n. 318 del 1999, ha avuto un effetto di stimolo e sensibilizzazione nei confronti degli utenti e del mercato nel suo complesso e non è da trascurare che è stato utile anche a formare una nuova cultura della sicurezza.

La revisione del regolamento sulle misure minime di sicurezza dovrà essere operata basandosi principalmente su due cardini:

- semplificazione del regolamento in modo tale da eliminare le difficoltà interpretative e ridurre la complessità del testo;

- rafforzamento delle misure minime di protezione dei dati vista la necessità di difendersi da comportamenti dolosi che si fanno progressivamente più sofisticati.

Pertanto, il regolamento andrà aggiornato tenendo presente nuovi aspetti della tecnologia, quali ad esempio, l'utilizzo ai fini della sicurezza dei nuovi sistemi che si basano sulle caratteristiche biometriche (geometria del volto, della mano, dell'iride, etc.). Il nuovo regolamento dovrà essere in grado di affrontare tematiche quali la costruzione e la gestione delle password nonché l'utilizzo dei Log, eliminando alcune parti dell'attuale disciplina che risultano essere oramai superate (quali ad esempio la differenza delle misure da adottare a seconda che le reti siano pubbliche o private) al fine di renderla più semplice ed attuale.

Concludendo, è necessario ma non è sufficiente avere un quadro generale di riferimento ove siano indicate norme comportamentali e relative sanzioni, ma va anche posta attenzione ad un altro aspetto importante: favorire la comprensione e la conoscenza delle tematiche della sicurezza e il rispetto dei valori etici nello sviluppo civile ed economico, promuovendo, fra tutte le parti in causa (pubbliche, private, studiosi della materia) la cooperazione e lo scambio di informazioni relative all'attuazione di politiche, procedure e misure di sicurezza. Per questo motivo ringrazio gli organizzatori per l'incontro di oggi che ritengo utile ad apportare quello scambio di esperienze necessario per raggiungere l'obiettivo comune di proteggere le informazioni che ci riguardano cioè di proteggere noi stessi, concretamente e nella nuova veste di "persone costituite da dati divulgati", dall'uso distorto che di questi dati potrebbe essere fatto.