FORUM P.A. 2001

I nuovi diritti nella Società dell'Informazione
Rispetto, qualità, trasparenza nel rapporto tra cittadini e P.A. dopo la legge sulla privacy

Mauro PAISSAN
(componente il Garante per la protezione dei dati personali)

Sono componente del Garante per la privacy da un mese e mezzo. Terrò conto io e terrete conto voi di questa circostanza, che non mi consente di intervenire sui primi quattro anni di attività del Garante, se non per dire che si è trattato di un'attività certamente meritoria e certamente di valore.

Per vent'anni ho fatto il giornalista (e si sa quanto la comunicazione abbia a che vedere, nel bene e nel male, con i diritti della persona), e per quasi dieci anni ho fatto il legislatore, agendo con nuove norme sulla carne viva dei diritti. La Pubblica Amministrazione sta nel mezzo di queste mie due attività: dipende dal Parlamento, ma anche dal ruolo di controllo e di critica dell'informazione. La Pubblica Amministrazione, insomma, fruisce e soffre di quelle che sono state la mie due attività.

Questo ho voluto dire solo per affermare che, da parecchi punti di vista, mi considero a casa come ambito tematico, nonostante il mio fresco arrivo al Garante. Mi limiterò comunque a una rapida comunicazione diretta a porre alcune questioni riguardo al rapporto tra privacy e processo di informatizzazione della P.A..

1. *Lo "stato dell'arte"*. Il dato dal quale muovere per lo svolgimento di queste schematiche e parzialissime osservazioni è l'irreversibile processo di "ristrutturazione" dell'architettura interna della pubblica amministrazione attraverso il massiccio ricorso all'informatica e alla telematica o, se si preferisce la locuzione inglese ormai entrata in uso comune, all'*Information & Communication Technology* (ICT). Processo già per larga parte attuato nel nostro ordinamento, e "fotografato" dall'ultima relazione dell'AIPA della quale, ancorché nel solo estratto, ho potuto prendere visione, ma più in generale in corso di svolgimento (con diversificati tempi di realizzazione) nel mondo occidentale e, per quanto più dappresso ci riguarda, all'interno dell'Unione europea [*Libro verde sull'informazione del settore pubblico nella società dell'informazione*].

Note sono altresì le cause che un po' dovunque hanno reso, oltre che opportuno, indilazionabile il ricorso all'ICT (anzitutto costi ed inefficienza delle P.A.), come pure le finalità perseguite: (con formula inevitabilmente sintetica) trasparenza, efficacia ed efficienza dell'azione amministrativa.

2. *Dall'*e-government *all'*e-citizenship. La panoramica appena tracciata rischia però di essere incompleta se non si menziona, da subito, l'ampio consenso dichiarato - seppure in tono minore - da parte dei *policy makers*

intorno alla necessità di rispettare i diritti fondamentali del cittadino scongiurando, con specifico riferimento alla protezione dei dati personali, il rischio di renderlo oltremodo "*trasparente*" di fronte alle pubbliche amministrazioni: basti, in questa sede, ricordare le recenti affermazioni di Franco Bassanini contenute nella Relazione introduttiva al III *Global Forum* di Napoli.

È questa, si badi, non una mera scelta di opportunità (se non, peggio, la risultante di un calcolo di convenienza), volta ad agevolare il definitivo incardinamento di ciò che, ellitticamente, definiamo *e-government.* Al contrario, si tratta di un imperativo derivante dalla Carta costituzionale che colloca al centro dell'ordinamento, riconoscendone la primazia, i valori della persona e della dignità personale; e giova altresì ricordare che in questa direzione, in modo ancora più esplicito, si muove il progetto della *Carta dei diritti fondamentali dell'Unione europea* (art. 8 Protezione dei dati di carattere personale), corrispondendo fra l'altro alle aspettative della stragrande maggioranza della popolazione nelle democrazie mondiali che, in qualsiasi indagine demoscopica, manifesta una generalizzata apprensione in ordine al rispetto della propria vita privata nella moderna era tecnologica (a fronte delle "intrusioni" provenienti sia dal settore pubblico che privato).

Ed allora, a mo' di prima conclusione, deve sottolinearsi che l'assunta centralità dell'*e-government* (specie se riducentesi ad un malinteso efficientismo) rischia di essere formula sviante in quanto monca o, peggio ancora, unilaterale se disgiunta dalla c.d. *e-citizenship*: merita, a questo riguardo, adesione lo spunto di Stefano Rodotà al *Global Forum* di Napoli. Non è casuale, dunque, il sottotitolo *«Toward an Electronic Citizenship»* della 22a Conferenza internazionale «*One World One Privacy*», organizzata dal Garante per la protezione dei dati personali a Venezia nel settembre 2000.

3. *Oltre l'affermazione di principio.* È, però, oltre che necessario, anche urgente (data la velocità con la quale l'ICT si va innervando nell'architettura amministrativa) procedere, da un lato, pur per linee generali, all'esame delle modalità e degli strumenti attraverso i quali *e-government* ed *e-citizenship* possano trovare armonica realizzazione; dall'altro, alla verifica, al di là delle dichiarazioni (o dei voti) di osservanza dei diritti fondamentali dei cittadini (sopra menzionate), del loro concreto rispetto nello svolgimento dell'agire amministrativo.

Prima di affrontare questi aspetti, solo una puntualizzazione (magari scontata) merita di essere fatta: in tanto l'*e-government* può doversi confrontare con la disciplina sul trattamento dei dati personali e, conseguentemente, rientrare nel raggio d'azione istituzionalmente proprio del Garante, in quanto si concreti in atti o attività che coinvolgano il trattamento di dati personali. La pubblicazione di norme in rete e di *forms*, dunque, pur integrando un'attività che con ragione può essere ricondotta nell'alveo *dell'e-government* (accentuando la trasparenza e l'efficienza dell'agire amministrativo), non solleva problemi nella prospettiva che qui interessa; i profili di *data protection* possono emergere,

invece, (in varia forma) rispetto alla c.d. reingegnerizzazione del processo amministrativo, che trova il suo punto di colmo con la realizzazione della rete unitaria della pubblica amministrazione (RUPA) e la conseguente circolazione all'interno di essa di informazioni personali dalla eterogenea provenienza.

In questo contesto non è, evidentemente, la pura e semplice accessibilità tecnica a giustificare, per sé sola, la circolazione delle informazioni; quest'ultima non può e non deve andare disgiunta dall'osservanza dei principi di *protezione dei dati*, primi fra tutti quelli di *finalità* e di *proporzionalità* nel trattamento dei dati personali, diversamente rilevanti, peraltro, a seconda della natura neutra o sensibile dell'informazione trattata.

Il menzionato processo di reingegnerizzazione dell'attività amministrativa non può dunque svolgersi indipendentemente dalla normativa sul trattamento dei dati personali; al contrario, essa viene a rappresentare un presupposto ineludibile dell'*e-governance*.

4. *L'obbligo di consultazione e il caso della tessera elettorale*. In quest'opera l'ordinamento ha predisposto uno strumento idoneo ad agevolare lo sviluppo dell'*e-government* nel rispetto dei diritti fondamentali della persona: si tratta dell'obbligo di consultazione del Garante, gravante in capo al Presidente del Consiglio dei Ministri e a ciascun ministro, «all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dalla legge [n. 675/1996]» (art. 31, 2° co., l. n. 675/1996).

Purtroppo, nonostante la (potrebbe dirsi, lungimirante) previsione legislativa, il Garante ha dovuto reiteratamente far rilevare alla Presidenza del Consiglio l'inosservanza del menzionato obbligo legale giungendo in ultimo a rendere pubblico, anche tramite il proprio sito web il rischio di annullabilità per violazione della legge sulla protezione dei dati dei regolamenti e degli atti amministrativi adottati senza la prescritta previa consultazione del Garante. Con l'ulteriore conseguenza che, integrando tale condotta in pari tempo una violazione del diritto comunitario, in caso di persistenza di detti inadempimenti il Garante si vedrà altresì costretto a renderne edotte le competenti autorità comunitarie.

Può altresì risultare istruttivo riflettere sulla circostanza che, al contrario, nelle ipotesi in cui la previa consultazione è avvenuta la stessa ha per lo più portato buoni frutti ed è stata valorizzata dalle singole amministrazioni, per quanto pure si siano dovuti registrare episodi nei quali il parere, pur richiesto, non è stato poi osservato; né si è trattato, vale la pena aggiungere, di violazioni di poco momento: volendo limitare i richiami alla mia brevissima esperienza al Garante è paradigmatico il recente caso delle tessere elettorali valide, come è noto, per 18 votazioni. Per quanto il ricorso ad esse sia stato, *peraltro a torto*, invocato al fine di elidere il rischio della (astratta) possibilità di esprimere due volte il diritto di voto da parte di una certa fascia dell'elettorato, oltre a conseguire significativi risparmi di spesa, è palese la loro idoneità ad incidere significativamente su diritti fondamentali del cittadino quali la

riservatezza di talune - magari assai intime - vicende personali (talora desumibili dalla sede della sezione), la libertà di voto (potendo rappresentare uno strumento improprio di "coazione" al voto) e finanche (pur indirettamente) la segretezza del voto (si pensi, ancora, ai casi di astensione dal voto nell'eventualità di referendum o ballottaggio). Rischi tutti tempestivamente rappresentati dal Garante, con la contestuale indicazione di soluzioni alternative, magari appena di là da venire (penso alla carta elettronica), ma ignorati dall'Esecutivo.

5. *La "valutazione di impatto sulla privacy". Alcuni esempi.* A chiusura di queste rapide notazioni sia consentito ritornare, con qualche esemplificazione, su uno degli aspetti che più puntualmente oggi ci occupa: il rispetto dei cittadino di fronte al nascente *e-government.*

Giacché se quella descritta è la cornice concettuale (se si vuole) che deve inscrivere (e così delimitare) il legittimo agire della P.A., non vorrei che la necessaria generalità della trattazione legittimasse in taluno il sospetto della sua vacuità o genericità: rischio sempre presente di fronte ad occasioni come quella odierna, specie di fronte alla reale novità del tema e all'innovatività delle applicazioni alle quali assisteremo nei prossimi anni.

Ma anche una rapida occhiata al panorama internazionale e una più attenta riflessione a taluna delle (in futuro sempre più numerose ed impreviste) applicazioni concrete dell'*e-government* contribuirà a fare giustizia di queste ipotesi.

Uno dei caratteri che sembra dover caratterizzare (non solo da noi) l'*e-government* è la presenza dell'accoppiata *front office/back office*, che dovrebbe consentire al cittadino, in condizioni di maggiore efficienza, la possibilità di ottenere un determinato servizio pubblico rivolgendosi ad una qualsiasi amministrazione di *front office* (si pensi esemplificativamente allo sportello unico delle imprese), luogo unitario nel quale si verifica una decentralizzazione multifunzionale. Evidenti ne sono i vantaggi, sia per il cittadino, sia per la P.A.: si tengano altresì presenti i rischi, però, atteso che la multifunzionalità implica inevitabilmente un incremento del flusso di informazioni personali, di natura eterogenea ed originariamente trattate dalle diverse branche dell'amministrazione, in un unico ufficio e, dunque, in ultima analisi, verso un ristretto gruppo di soggetti che in questo ufficio svolgono il proprio compito e che, pertanto, possono realmente pervenire ad un quadro completo del cittadino, in quanto "ricomposto" rispetto alle diverse identità che la tradizionale ripartizione verticale dei flussi informativi per settori consentiva.

Di questa nuova prospettiva dovrà pur tenersi conto anche con l'introduzione di congrue misure tecniche ed organizzative (magari con una separazione interna) degli stessi *front offices*, considerandone altresì l'opportuna distribuzione sul territorio (affinché non risultino serventi di comunità troppo piccole) e contemplando altresì, specie se i dati coinvolti hanno natura sensibile (si pensi ai dati sanitari, ma è solo un esempio) la possibilità di scelta del

cittadino di rivolgersi alla tradizionale struttura "verticale" escludendo la (inesorabile) logica dell'*one-stop shop.*

Rimanendo con il pensiero alla struttura del *front office* non può che pensarsi anche alla, forse banale, collocazione spaziale entro la quale le informazioni personali (in ipotesi di svariata natura) debbono essere raccolte e trattate, con la conseguente necessità di dotarsi di strutture adeguate che consentano di trattare (preferibilmente) "a quattr'occhi" le pratiche, almeno quelle più delicate.

***

Ma l'*e-government* è formula ampia, idonea a comprendere l'offerta di taluni servizi anche per via telefonica, magari ricorrendo all'opera di *call centers* avvalendosi delle moderne tecniche dell'*out-sourcing* (si pensi ad es. a centri ospedalieri - grandi o piccoli - che intendano far gestire secondo detto modulo organizzativo il servizio di prenotazione dei servizi sanitari): si pone qui un problema d'informazione del cittadino che all'apparecchio può ignorare l'effettiva natura dell'interlocutore telefonico, come pure della amministrazione che, nell'esternalizzare dette attività, deve opportunamente disciplinare la relazione contrattuale prestando adeguata attenzione ai profili di *data protection*.

***

Nell'era dell'amministrazione *on-line* problemi di tutela dei dati personali si pongono, poi, non solo per i cittadini, ma anche per gli stessi dipendenti pubblici che possono vedere i propri dati personali, ad iniziare dal proprio nominativo, inseriti in rete e dunque, soggetti ad un'ampia circolazione oltre che esposti alla più rapida individuazione tramite i sempre più potenti motori di ricerca: anche qui si dovrà operare solo in presenza di un'adeguata previsione normativa ed ispirandosi al principio della necessità nel trattamento di dette informazioni personali.

***

Ancora un esempio di vivissima attualità: il ricorso alle *web cams* per le più svariate applicazioni, ad esempio per il controllo delle condizioni del traffico. Anche qui potrebbe darsi un inutile trattamento di dati personali (ad es. dell'immagine di persone che transitano) rispetto alla finalità perseguita ed ottenibile ad un costo (in termini di protezione della *privacy*) più basso (ad es. valendosi di riprese in campo lungo che consentono comunque il perseguimento della finalità voluta).

6. *Alcune conclusioni*. Le esemplificazioni si possano moltiplicare e l'elenco diverrebbe, credo, assai lungo: confido, tuttavia, di avere messo in luce in tutta concretezza i rischi effettivi, ben lungi dall'essere solo preoccupazioni di chi della *privacy* deve occuparsi istituzionalmente, ai quali il cittadino andrà comunque incontro di fronte all'utilizzo delle *information & communication technologies.*

Nel proprio svolgersi l'attività della P.A., ancorché "reingegnerizzata" ed anzi proprio nel corso del processo di reingegnerizzazione, non potrà dunque prescindere dalla previa "valutazione d'impatto sulla privacy" dei

cittadini (prendo a prestito la formula utilizzata da Flaherty alla conferenza di Venezia) e dal rispetto della dignità della persona come valore fondativo della stessa azione amministrativa e limite alle conseguenze negative - magari inconsapevolmente introdotte - della rincorsa tecnologica.