La protezione dei dati tra libertà e sicurezza[1]

Francesco Pizzetti[2]

Vi ringrazio per avermi invitato ad intervenire a questo incontro che costituisce una preziosa occasione per confrontarci su tematiche che coinvolgono la protezione dei dati nella ricerca di un bilanciamento tra uomo e tecnica, tra società in continua evoluzione e capacità di adattamento dell'individuo.

Colgo l'occasione per esporre in modo più compiuto una materia delicata e complessa, caratterizzata dalla grande trasversalità dei settori su cui il Garante, che ho l'onore di presiedere da quasi un biennio, è chiamato a intervenire.

Sono trascorsi dieci anni dall'entrata in vigore nel nostro ordinamento della normativa in materia di protezione dei dati personali. La prima fase di attività dell'Autorità è stata preordinata alla formazione di quella che potrebbe definirsi "cultura della privacy". Da poco è stata inaugurata una seconda fase, caratterizzata dall'impegno di "modernizzare" il settore della protezione dei dati adattandolo alle esigenze di una società in continuo cambiamento tecnologico e sociale.

Gli episodi degli ultimi anni, e, in particolare quelli correlati alle attività di dossieraggio, intercettazioni telefoniche, accesso alle banche dati -dalla banca dati di traffico telefonico a quella dell'anagrafe tributaria- dimostrano il vero ruolo di questa Autorità, chiamata a vigilare e accompagnare la crescente espansione del fenomeno del trattamento dei dati personali.

Mi auguro, pertanto, che, prima o poi, la vecchia battuta «Mettete una firma per la privacy» sia consegnata alla memoria. Infatti, a seguito di un approccio incentivato erroneamente, il concetto di privacy è stato ricondotto essenzialmente ad un fatto burocratico. Solo di recente, invece, si inizia a comprendere, e vorrei che tale consapevolezza fosse sempre più diffusa, che la protezione dei dati costituisce un valore essenziale.

Ritengo che oggi sia più rischioso un utilizzo illecito dei nostri dati personali rispetto al furto del nostro portafogli. Si pensi, inoltre, a cosa può determinare l'accesso ai dati di una cartella clinica o l'acquisizione del traffico telefonico di un individuo con la mappatura completa di tutte le sue comunicazioni.

Siamo inevitabilmente portati a produrre dati e questo è un fenomeno destinato a crescere in misura sempre più significativa anche attraverso l'ausilio delle moderne tecnologie che agevolano la raccolta di informazioni. Questi dati, infatti, sono incrociabili e trattabili con estrema facilità e rapidità, perché possono essere

---

1 Sbobinatura rivista dall'autore della relazione tenuta il 2 dicembre 2006 al Convegno "Più liberi o più sicuri? Le sfide della privacy nell'età globale" organizzato dal Cespec – Cuneo.

2 *Presidente dell'Autorità Garante per la protezione dei dati personali*

trasferiti su supporti informatici, di norma telematici, ed elaborati con programmi che la nostra sociologia e la nostra scienza informatica tendono a moltiplicare.

Si pensi, infatti, alle innumerevoli quantità di dati e di immagini rilevate dalle videocamere nei luoghi pubblici: solo nel centro di Londra si calcola che esistano 5000-6000 videocamere su un percorso di un normale tragitto urbano. Per altro verso, e poi concludo questa trattazione introduttiva, occorre ricordare che anche un solo dato, o una singola serie di dati può rivelare una ricchissima quantità di informazioni. Ad esempio, un grande magazzino, con una carta di fidelizzazione e la successiva registrazione degli acquisti, è in grado di ricostruire le abitudini di un cliente, il reddito, il nucleo familiare, i gusti. Con alta probabilità, infatti, l'acquisto di una confezione di pannolini indicherà la presenza di bambini piccoli nella famiglia del cliente fidelizzato mentre l'acquisto di prodotti senza sale indicherà che l'acquirente segue una dieta iposodica.

Pertanto, si può dire che aderire ad una carta di fidelizzazione equivale ad accettare che il commesso di un grande magazzino venga in casa nostra, apra il frigorifero, gli armadi, gli sportelli, e sappia assolutamente tutto di noi.

Spostando ora l'analisi alla normativa sulla protezione dei dati, deve in primo luogo evidenziarsi che il nostro ordinamento ha previsto una disciplina differenziata a fronte della natura giuridica che qualifica il soggetto attivo del trattamento.

In generale, nei rapporti tra privati deve considerarsi illecito ogni trattamento di dati che avvenga senza il consenso dell'interessato. Non è consentito, infatti, utilizzare un dato personale se il soggetto cui esso si riferisce non abbia espresso un consenso consapevole e preventivamente informato in ordine alla modalità e alla finalità del suo utilizzo.

Tale volontà viene comunemente acquisita, anche nei casi in cui il consenso non deve manifestarsi in forma scritta, mediante la c.d. "firmetta per la privacy" che, solitamente, è alla base di una informativa lunghissima, di cui spesso non si comprende il significato.

Invero, questa impostazione costituisce il nostro tallone d'Achille poiché si sostanzia in un fatto puramente burocratico che sostanzialmente lascia i soggetti privi di tutela.

Spostando l'interesse all'analisi del trattamento in ambito pubblico, deve rilevarsi che la P.A., perseguendo interessi e finalità istituzionali fissati dal legislatore, il c.d. "fine pubblico", può effettuare esclusivamente i trattamenti di dati connessi all'esercizio delle proprie funzioni istituzionali senza dover acquisire il consenso degli interessati.

Pertanto, nell'ambito dei trattamenti effettuati dalla Pubblica Amministrazione, la tutela del cittadino appare edulcorata e, dunque, è importante che in tale settore si diffonda maggiormente la cultura della protezione dei dati.

La P.A., infatti, tratta continuamente dati sensibili dei cittadini. Le prestazioni in materia socio-sanitaria contengono necessariamente dati sulla salute. Si pensi poi a tutte le altre prestazioni che possono correlarsi ad attività politiche, sindacali, ecc.

Inoltre, l'innovazione tecnologica, attraverso la moltiplicazione di reti e

archivi informatici, sta determinando una profonda trasformazione nella Pubblica Amministrazione. Se è forte la tentazione efficientista ad interconnettere tali sistemi fra di loro, è altrettanto alto il rischio di determinare una circolazione incontrollata dei dati e l'accesso indiscriminato da parte degli operatori.

Il Garante ha affrontato tale fenomeno a partire dalla complessa vicenda nota come "Laziomatica". Presso Laziomatica S.p.a. (società per azioni a prevalente capitale regionale istituita dalla Regione Lazio che le ha affidato la gestione del Sistema informatico regionale) sono stati effettuati, su richiesta di un avvocato, alcuni accessi illeciti al data base anagrafico del Comune di Roma che la Regione era stata autorizzata a consultare solo per alcune finalità sanitarie, sulla base di un Protocollo di intesa. Addetti della società hanno effettuato ripetuti accessi a dati personali, riguardanti anche documenti di identità, per verificare l'irregolarità di alcune sottoscrizioni di liste di candidati alle elezioni regionali.

L'Autorità ha accertato la violazione degli obblighi e delle garanzie previsti dal Codice in materia di protezione dei dati personali a seguito di accertamenti estesi alla sicurezza dei dati presso i data-base anagrafici del Comune, al quale sono stati prescritti adempimenti tecnici e misure riguardanti la sicurezza dei dati e la gestione del sistema informatico anagrafico.

La Pubblica Amministrazione se può trattare i dati senza consenso, ha però il dovere di proteggerli e di fornire idoneo riscontro al cittadino che esercita il diritto di accesso alle proprie informazioni.

Tuttavia, le regole generali che disciplinano i trattamenti effettuati in ambito pubblico incontrano talune limitazioni nei settori Giustizia e Sicurezza.

Infatti, ai trattamenti effettuati per ragioni di giustizia non si applicano molti tra i principali articoli del Codice poichè le regole fondamentali per il trattamento dei dati nei processi sono implicitamente contenute nei Codici di Procedura.

Non trova, ad esempio, applicazione la norma che consente all'interessato di rivolgere direttamente al titolare del trattamento un'istanza per far valere i suoi diritti.

L'interessato però non rimane privo di tutela nei confronti dei dati che vengono trattati in ambito processuale, avendo comunque la possibilità di rivolgersi al Garante con una segnalazione o con un reclamo o all'autorità giudiziaria, azionando la procedura ex art. 152 del Codice.

Analoghe eccezioni alle regole generali trovano applicazione ai trattamenti posti in essere dalle forze di polizia. In tale ambito, infatti, solo i trattamenti effettuati dal CED (Centro elaborazione dati del Dipartimento di pubblica sicurezza) restano disciplinati dai principi generali del Codice.

Il discrimine tra settore pubblico e privato fa emergere un ruolo sempre più significativo del Garante che nei settori Giustizia e Sicurezza è ancora più rilevante.

Si pensi alla tematica concernente la "sicurezza" della conservazione dei dati personali raccolti e dei flussi informativi contenuti nelle banche dati di traffico nell'ambito delle telecomunicazioni, con particolare riferimento alle attività svolte per le intercettazioni disposte dalla magistratura.

Con due provvedimenti il Garante ha prescritto ai principali fornitori, cui compete lo svolgimento di servizi per conto dell'autorità giudiziaria, di adottare un modello organizzativo in grado di limitare al minimo la conoscibilità delle informazioni relative alle attività svolte per esigenze di giustizia, con una rigida partizione della visibilità dei dati su base organizzativa, funzionale e di area geografica di competenza.

Si pensi, altresì, alla attuale disciplina in tema di *data retention* dettata dall'art. 132 del Codice. A tale riguardo, il legislatore ha demandato al Garante l'individuazione di specifiche misure ed accorgimenti da porre a garanzia degli interessati con riferimento ai dati relativi al traffico telefonico e telematico che devono essere conservati dai fornitori di servizi di comunicazione elettronica per finalità di accertamento e repressione di reati e che possono essere resi conoscibili secondo le modalità regolate dal Codice di procedura penale.

Per quanto concerne il dibattito correlato al rapporto tra privacy e sicurezza, stamani si è tentato di individuarne il punto di equilibrio.

Sicurezza e privacy possono costituire due aspetti apparentemente antitetici con cui le società occidentali sono costrette a rapportarsi quotidianamente al fine di stabilire volta per volta quale dei due debba ricevere una minore o maggiore tutela. A fronte della più recente giurisprudenza del Garante, deve evidenziarsi che la sicurezza, abbinata all'uso delle tecnologie, che rappresentano il più moderno terreno su cui saggiare il livello di tutela della riservatezza, ben si raccorda con la tematica della protezione dei dati, purché ciò avvenga nel rispetto delle regole fissate dall'Autorità di garanzia.

In realtà sarebbe necessario un dibattito pubblico serissimo su quali siano i dati veramente necessari a fini di sicurezza, sapendo che esiste un grado di tecnicità che sfugge a tutti noi, se non siamo esperti di sicurezza, e anche un dato di politicità, ossia di scelte che una società deve fare e che non può essere trascurato. Del resto, in un momento storico in cui manca ogni capacità di dare una risposta politica alle vicende terroristiche e in cui l'Europa e gli Stati Uniti, ma soprattutto l'Europa, delegano alle strutture di sicurezza il compito di garantirla, inevitabilmente tali organismi tendono ad acquisire sempre maggiori informazioni sulle persone.

Ma, pur accettando ogni controllo dagli organi preposti alla sicurezza del mio Paese, è, tuttavia, necessario che si riceva in cambio la certezza che i dati raccolti vengano utilizzati unicamente per le finalità istituzionali e vengano protetti da accessi illeciti. Quindi, quanto più si afferma che per ragioni di sicurezza o di controllo fiscale o di giustizia occorrono più dati, tanto più cresce il diritto dei cittadini di esigere che tali dati siano correttamente protetti.

Concludo il mio intervento con alcune considerazioni in materia di intercettazioni telefoniche. Non entro nel merito di una valutazione sull'opportunità di ricorrere troppo spesso o troppo poco alle intercettazioni legittime, poiché siamo un Paese ad alta criminalità che va senz'altro contrastata. Le intercettazioni legittime sono palesemente quelle, e solo quelle, che i magistrati richiedono per fini di giustizia, nei casi previsti dal Codice di Procedura Penale. Se sono eccessive è un

problema dei giudici; se sono molte le fattispecie di reato che ammettono il ricorso a tale strumento è, invece, un problema del legislatore.

E' però fondamentale che le informazioni relative ai soggetti intercettati siano protette. Le intercettazioni telefoniche non riguardano solo la magistratura, ma anche i gestori che mettono la magistratura in grado di conoscerne il contenuto e gli operatori che materialmente le effettuano e le trascrivono. Siamo intervenuti da un paio di anni su questa tematica e posso dire, con un certo orgoglio, che questo è uno dei settori in cui siamo più avanti e che siamo oggi il soggetto pubblico più esperto in materia di tutela delle grandi banche dati che ci sia in Italia. Abbiamo adottato una serie di provvedimenti nei confronti dei gestori, di cui l'ultimo dovrà concludersi entro il 31 dicembre 2006, che prescrivono l'adozione di efficaci misure per la sicurezza di tali delicate informazioni.

Dal marzo scorso, con due comunicazioni indirizzate al CSM e al Ministro della Giustizia, reiterate al nuovo Ministro e al nuovo CSM, stiamo chiedendo anche agli uffici giudiziari efficaci protocolli di sicurezza.

Cosa ben diversa è, invece, definire se l'intercettazione depositata in Cancelleria sia conoscibile al giornalista e se possa essere pubblicata, ma mettere in sicurezza gli uffici giudiziari vuol dire evitare fughe illecite di notizie quando il dato è a disposizione dell'Autorità Giudiziaria. Si sono, infatti, verificati numerosi casi in cui l'intercettazione, seppur lecita, è stata utilizzata da soggetti non autorizzati. La famosa telefonata tra Consorte e Fassino è un caso classico di intercettazione lecita, usata in modo illecito, mentre era ancora nella piena disponibilità delle Autorità Giudiziarie e dell'Autorità di Polizia Giudiziaria incaricata dal magistrato di conservare il dato. L'Autorità Giudiziaria ha, dunque, un dovere qualificato di mettere in atto tutte le misure necessarie a proteggere i dati dei cittadini, non solo perché ha il dovere di tutelare la privacy dei cittadini ma anche perché se il contenuto di un'intercettazione viene diffuso illecitamente risulta vanificato uno strumento di indagine investigativa che il nostro ordinamento mette a sua disposizione.