GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione 2002

Discorso del Presidente
Stefano Rodotà

Roma, 20 maggio 2003

www.garanteprivacy.it

Signor Presidente della Repubblica,

due tendenze, spesso contrapposte, hanno dominato nell'ultimo anno il mondo della protezione dei dati personali. Riconosciuta come diritto fondamentale dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, la protezione dei dati personali vedrà confermata e rafforzata questa sua natura dal futuro Trattato costituzionale dell'Unione europea. Emerge una nuova dimensione della libertà dei contemporanei, fondata sulla "costituzionalizzazione" della persona. Un modello, creato nell'Unione europea, sta diventando punto di riferimento per i più diversi paesi del mondo, dando così un contributo importante alla "globalizzazione attraverso i diritti".

Al tempo stesso, però, si è fatta più massiccia la pressione per utilizzare qualsiasi dato personale soprattutto per ragioni di sicurezza interna e internazionale, ma anche per finalità commerciali, né si è spenta la resistenza di molti settori della pubblica amministrazione. E l'incessante innovazione scientifica e tecnologia, che congiunge campi fino a ieri lontani come l'elettronica e la genetica, sembra rendere vana ogni pretesa di offrire tutele giuridiche.

Come si governa questa realtà variegata e contraddittoria, questo continuo divaricarsi tra il rafforzamento delle tutele istituzionali e le pretese di non tenerne conto? Bisogna rifuggire da impostazioni che presentino come inevitabilmente conflittuali il diritto alla protezione dei dati personali ed altri diritti. E analizzare piuttosto le dinamiche reali, dove il gioco degli interessi rifiuta d'essere chiuso in schemi semplificati.

Le invasioni quotidiane della sfera privata

Lo dimostra con chiarezza una vicenda recentissima, quella dell'invio massic-

cio di messaggi non desiderati di posta elettronica. Il Garante italiano ha sempre sostenuto che invii del genere fossero legittimi solo con il consenso degli interessati: un atteggiamento che qualcuno giudicò eccessivo, arrivando addirittura a parlare di un "*khomeinismo*" del Garante.

Ma la nostra posizione ha poi trovato conferme in atti come la Direttiva europea 58/02, in occasione della quale la scelta per l'opt-in, per il consenso degli interessati, ha prevalso grazie anche al sostegno del ministro delle Comunicazioni. E vi è, eloquentissima, la forza delle cose. Improvvisamente gli Stati Uniti hanno scoperto che lo *spamming*, l'invio massiccio di "messaggi spazzatura", ha ormai superato il 40% del traffico su *Internet*, passando da un miliardo di messaggi nel 1999 a 5.6 miliardi nel 2002. La Federal Trade Commission accerta che il 66% di questi messaggi contiene "elementi di falsità", percentuale che arriva al 90% per le offerte finanziarie o di investimento. Sommersa dalle proteste, la più grande società del settore, America on Line, chiede dieci milioni di dollari di risarcimento a cinque società responsabili di *spamming*, seguendo l'esempio di altre imprese che già hanno ottenuto risarcimenti miliardari. E si calcola che lo *spamming*, nel 2002, sia costato all'economia americana quasi 9 miliardi di dollari.

Con uno spettacolare rovesciamento di posizioni, il paese più ostile alla regolamentazione della rete ha imboccato la via di pesantissimi interventi legislativi. Lo Stato della Virginia ha approvato una legge che considera l'invio massiccio di posta elettronica indesiderata come un reato, punibile con la reclusione da uno a cinque anni. Il Congresso affronterà questo problema, considerando anche la possibilità di "taglie" a favore dei cacciatori di chi fa *spamming*.

Ha dunque ragione l'Europa nel ritenere indispensabile l'uso dello strumento legislativo per la concreta protezione dei dati personali, e per evitare che la natura stessa di *Internet* sia stravolta da una sua trasformazione in un gigantesco contenitore di messaggi spazzatura. In questa materia interveniamo quasi quotidianamente

a tutela dei cittadini vittime dello *spamming*; abbiamo sottolineato che la semplice presenza in rete di un indirizzo di posta elettronica non lo rende "pubblico", utilizzabile senza il consenso dell'interessato; abbiamo già bloccato una ventina di banche dati utilizzate a questo fine, con interventi finora unici in Europa e che intensificheremo già nelle prossime settimane. Ci muoviamo lungo una linea che, dando piena tutela alla sfera privata, può evitare in futuro derive costose per il sistema economico, testimoniate dall'esperienza americana e da una circolazione globale quotidiana di 30 miliardi di *e-mail* al giorno. Cominciamo così a tradurre in azione concreta il titolo di un nostro seminario internazionale del dicembre passato, quando avevamo parlato di una *privacy* che da costo si faceva risorsa. Possiamo dire di essere stati più lungimiranti di molti imprenditori indicando nell'invio massiccio di messaggi indesiderati una malattia che avrebbe potuto pregiudicare la salute del sistema imprenditoriale.

Si affronta così una emergenza concreta, e al tempo stesso si dà rilievo ad una questione più generale. Oggi la tutela dei dati personali non riguarda soltanto la divulgazione impropria delle nostre informazioni. Consiste anche nella difesa della sfera privata contro invasioni che violano il diritto alla tranquillità, cancellano il diritto di non sapere.

Uno Stato, una privacy

Quando altre esigenze premono, come accade oggi con quelle legate alla sicurezza interna ed internazionale, il bilanciamento tra gli interessi deve sempre assicurare il mantenimento di un "elevato grado di tutela", come vuole la Direttiva 95/46. Nelle passate relazioni abbiamo richiamato molti casi nei quali il nostro intervento ha reso possibile la coesistenza tra le ragioni della sicurezza e quelle della tutela dei dati personali. Oggi ricordiamo che la Carta dei diritti fondamentali dell'Unione europea obbliga a rispettare il contenuto essenziale dei diritti (art.

52.1) e che la Convenzione europea dei diritti dell'uomo prevede la possibilità di limitazioni alla tutela della vita privata, ma le subordina in ogni caso al fatto che si tratti di misure necessarie "in una società democratica".

La difesa del valore della democrazia, dunque, appare il bene da salvaguardare prima di ogni altro. Il Garante non è certo l'unica istituzione alla quale sia stato affidato il compito di evitare che le nostre divengano quelle società della sorveglianza e della classificazione delle quali già in passato avevamo paventato l'avvento. Ma nell'ultimo periodo questo rischio è aumentato, si è fatto sempre più evidente l'intreccio tra questione democratica e tutela dei dati personali.

Questo ci attribuisce una maggiore responsabilità, accresce quel carattere di istituzione di frontiera che il Garante, fin dall'origine, ha avuto. Possiamo contribuire a far sì che nei momenti difficili non prendano il sopravvento reazioni emotive o interessate, che inducano a scambiare libertà della sfera privata contro sicurezza, invece di ricercare i possibili punti di equilibrio, rispondenti alla logica che ha ispirato il testo di base in questa materia, la Direttiva europea 95/46, che ha garantito, al tempo stesso, la massima possibile circolazione delle informazioni personali e la massima loro tutela. Questo vuol dire che ogni misura che incide sulla tutela dei dati personali deve sempre essere accompagnata da controlli e garanzie ulteriori, in grado di salvaguardare appunto gli equilibri democratici.

Il nostro compito sarà certamente reso più incisivo dalla prossima approvazione del codice per la protezione dei dati personali, attualmente all'esame delle Camere e che, non a caso, si apre riproducendo il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea: "Chiunque ha diritto alla protezione dei dati di carattere personale che lo riguardano". Non è un omaggio formale. È la conferma della natura nuova che il diritto alla tutela dei dati personali ha definitivamente assunto, dando piena evidenza ad un sistema di garanzie che deve accompagnare la persona in ogni momento di una vita divenuta ormai uno

scambio continuo di informazioni, una rappresentazione sociale che dà pubblica e continua evidenza al corpo e alle sue immagini, alle opinioni ed alle preferenze, ai narcisismi ed al pudore.

È nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il forte diritto di non perdere mai il potere di mantenere il pieno controllo sul proprio "corpo elettronico", distribuito in molteplici banche dati, nei luoghi più diversi. Un diritto che si caratterizza ormai come componente essenziale della nuova cittadinanza, da intendere come il fascio di poteri e doveri che appartengono ad ogni persona, e non più come il segno d'un legame territoriale o di sangue.

Questa ricostruzione della natura della tutela dei dati personali non risponde soltanto ad una esigenza di pulizia concettuale. Ha immediate implicazioni istituzionali. Come diritto fondamentale della persona, ed elemento costitutivo della sua cittadinanza, la tutela dei dati personali si colloca tra le materie per le quali lo Stato mantiene competenza legislativa esclusiva, nel quadro già disegnato dalla riforma del Titolo V della Costituzione e confermato dai riferimenti all'"unità giuridica" ed all'"interesse nazionale" contenuti nei testi attualmente all'esame delle Camere, giustamente ispirati al criterio che vuole i diritti fondamentali sottratti al rischio di disarmonie territoriali e, nel nostro caso, affidati quindi alla garanzia di una sola autorità indipendente.

La questione già si è posta concretamente in occasione di una legge della provincia di Bolzano (15 novembre 2002, n. 14) istitutiva di una banca di dati in materia sanitaria, che il Consiglio dei ministri, nella riunione del 24 gennaio 2003, ha opportunamente impugnato davanti alla Corte costituzionale, sottolineando che "la tutela della *privacy*, classico esempio di diritto inviolabile, non può non essere rimessa alla competenza dello Stato". E si è anche ricordato che si deve considerare "principio fondamentale della materia" la disposizione conte-

nuta nell'art. 23.4 della legge sulla protezione dei dati personali, che vieta la rivelazione dei dati sulla salute, salvo che ciò sia necessario per l'accertamento, la prevenzione e la repressione dei reati. Inutile dire che la decisione della Corte assumerà particolare rilevanza non solo per la definizione delle competenze di Stato, Regioni e province autonome (il problema già si pone per diverse regioni), ma anche per un chiarimento di portata generale sulla possibilità, da parte di soggetti pubblici, di trattare i dati sulla salute per finalità diverse da quelle della diretta tutela dell'interessato.

È opportuno ricordare che più volte il Garante ha dato una interpretazione rigorosa delle norme in materia, quando si intendeva ricorrere a dati sulla salute per realizzare, ad esempio, finalità di lotta all'evasione fiscale. Intendiamo tener fermo questo orientamento, anche per evitare violazioni del fondamentale principio dell'eguaglianza tra i cittadini. Se, ad esempio, si costituissero banche dati contenenti tutte le prescrizioni mediche con indicazione nominativa delle persone alle quali si riferiscono, si creerebbe un sistema ad alto rischio sociale, al quale potrebbero sottrarsi soltanto coloro i quali decidessero di non utilizzare il sistema sanitario nazionale e di pagare direttamente i farmaci. Non permetteremo la trasformazione della protezione dei dati personali in un privilegio per i più abbienti.

Corpo, salute, dignità: la genetica come questione centrale

I dati sulla salute richiedono sempre una attenzione particolare, non solo perché così vuole la legge, ma perché essi rimandano alla nuda condizione umana, colgono la persona nei momenti di massima fragilità, rivelano la debolezza del corpo. E proprio il corpo, quello fisico e non quello disincarnato delle informazioni elettroniche, è oggi al centro di una attenzione che vuole scandagliarne ogni recesso, utilizzarne ogni possibilità. Qui l'intreccio tra elettronica, biologia e genetica ha già aperto scenari nuovi, insieme promettenti e inquietanti. Qui si gioca una partita

essenziale per il futuro della protezione dei dati, la cui intensità diviene anche la condizione perché ciascuno possa godere delle grandi promesse della genetica.

Il corpo sta diventando una *password*, la fisicità prende il posto delle astratte parole chiave, impronte digitali, iride, tratti del volto, Dna: si ricorre sempre più frequentemente a questi dati biometrici non solo per finalità di identificazione o come chiave per l'accesso a diversi servizi, ma anche come elementi per classificazioni, per controlli ulteriori rispetto al momento dell'identificazione. E il corpo può essere predisposto per essere seguito e localizzato permanentemente. Alcuni genitori inglesi, traumatizzati da rapimenti e violenze sui bambini, hanno chiesto che sotto la pelle dei loro figli venga inserito un *chip* elettronico proprio per poter sapere in ogni momento dove si trovano. La sorveglianza sociale si affida ad una sorta di guinzaglio elettronico, il corpo umano viene assimilato ad un qualsiasi oggetto in movimento, controllabile a distanza con una tecnologia satellitare.

Le derive tecnologiche assumono così tratti particolarmente inquietanti. Le finalità di identificazione, sorveglianza, sicurezza delle transazioni possono davvero giustificare qualsiasi utilizzazione del corpo umano resa possibile dall'innovazione tecnologica?

La nostra linea di lavoro su questi temi può essere così sintetizzata:

- rispetto della dignità della persona, espressamente richiamata dall'art. 1 della legge n. 675 del 1996 e dichiarata inviolabile dal primo articolo della Carta dei diritti fondamentali dell'Unione europea;

- rispetto dell'identità personale, anch'essa menzionata nell'art. 1 della legge, considerando in particolare i possibili "furti d'identità", già ricordati nella Relazione dello scorso anno a proposito delle impronte digitali e che

diventano pericolosissimi quando riguardano il materiale genetico e le relative informazioni;

- rispetto dei principi di finalità e di proporzionalità: solo ragioni sociali molto forti, e non una semplice convenienza organizzativa o economica, possono giustificare il ricorso alla biometria, che tuttavia non deve essere utilizzata per schedature centralizzate e di massa e deve sempre essere accompagnata da adeguati strumenti di controllo affidati anche agli stessi interessati;

- attenzione per gli effetti cosiddetti imprevisti o indesiderati e che, invece, spesso sono conseguenze determinate da analisi incomplete o troppo interessate delle tecnologie alle quali si intende ricorrere.

Il problema della protezione dell'identità dai suoi possibili "furti", già imponente nel settore del commercio elettronico e che esige cautele particolari per le impronte digitali, può divenire drammatico se il furto riguarda materiale che consente di ottenere informazioni genetiche. Un recente caso di cronaca può illustrare la questione in modo semplice e persuasivo. Una persona ben nota è stata seguita, e ci si è impadroniti di un suo fazzoletto di carta buttato via dopo essersi soffiato il naso. Il materiale genetico così raccolto è stato poi adoperato, ovviamente all'insaputa dell'interessato, per effettuare accertamenti riguardanti la sua paternità.

La violazione della sfera privata, in sé gravissima, diviene ancor più inquietante se si tiene conto del fatto che, grazie ai dati ricavabili da qualsiasi frammento di materiale genetico (saliva, capelli, pelle, sangue), è possibile ottenere informazioni relative non soltanto all'identità della persona, ma anche di tipo "predittivo". E, poiché il genoma costituisce il tramite tra le generazioni, i dati riguardanti una singola persona forniscono informazioni su tutti gli appartenenti al suo gruppo biologico. Passato, presente e futuro, dunque, possono essere scan-

dagliati attraverso i dati genetici. Riteniamo che, in un tempo in cui si puniscono con severità eccessiva violazioni della proprietà intellettuale, i legislatori debbano riflettere su questa possibilità di impadronirsi di un aspetto dell'identità altrui che tocca le radici stesse dell'esistenza individuale e di gruppo, prevedendo anche una adeguata tutela penale.

Verrebbe così efficacemente integrato un sistema di tutela dei dati necessario anche per consentire a tutti di godere al massimo dei benefici della ricerca genetica. Benefici grandi, che ampliano le possibilità di prevenzione e di cura di un numero crescente di malattie, di trattamenti farmacologici personalizzati, in generale di compiere scelte di vita in modo più consapevole. Ma la condizione prima di questo arricchirsi della libertà e della tutela della salute è un ricorso ai dati genetici strettamente limitato alle finalità prima indicate. L'esperienza internazionale ci dice che le persone spesso preferiscono rinunciare ai benefici loro offerti dalla genetica se temono che i loro dati possano poi essere utilizzati da altri in modo discriminatorio. Questo è, appunto, uno di quegli effetti "imprevisti" che, invece, sono facilissimi da prevedere e che è compito di una istituzione come la nostra evitare.

Le nuove diseguaglianze

Se, infatti, grandi sono le opportunità offerte dalla genetica, altrettanto grandi sono i rischi di utilizzazioni dei dati genetici che possono determinare discriminazioni nell'accesso al lavoro o al credito, nella conclusione di contratti di assicurazione vita o malattia, o attraverso forme di schedatura genetica di massa. Non a caso tutti i documenti internazionali sottolineano con forza questo aspetto. "È vietata qualsiasi forma di discriminazione fondata, in particolare, (…sul)le caratteristiche genetiche" – dice l'art. 21 della Carta dei diritti fondamentali dell'Unione europea. Si vieta "ogni forma di discriminazione nei confronti di una persona per il suo patrimonio genetico" nell'art. 11 della Convenzione europea di biomedicina.

E lo stesso orientamento si trova nell'art. 6 della Dichiarazione universale sul genoma umano: "nessuno può essere discriminato per le sue caratteristiche genetiche, con finalità o effetti di violazione dei suoi diritti e libertà fondamentali e del riconoscimento della sua dignità".

È indispensabile, quindi, non solo impedire iniziative che possano nell'immediato provocare discriminazioni, ma anche evitare che si creino situazioni comunque propizie alla diseguaglianza. Il nostro immediato programma d'azione è volto a controllare la legittimità di ogni forma di trattamento dei dati genetici; a ribadire la rilevanza dell'informazione e del consenso degli interessati; a valutare i contesti all'interno dei quali si svolge l'attività di raccolta e trattamento dei dati genetici, riprendendo in particolare l'attività di controllo sui progetti di ricerca genetica sulle popolazioni, già in corso in diverse regioni; a seguire con il massimo rigore gli intrecci nuovi tra tecnologie informatiche e trattamento dei dati genetici.

Denunciamo senza ambiguità il grave rischio rappresentato dall'offerta di *test* genetici via *Internet*. I genetisti li condannano, così come diverse organizzazioni per la tutela dei diritti civili; serissime riserve sono state espresse dalla *Human Genetics Commission* inglese, in un rapporto del marzo di quest'anno. Le tecniche adoperate accrescono le preoccupazioni. I *test* vengono spesso proposti come se si trattasse di un qualsiasi prodotto da supermercato: paghi due e scegli tre *test* in un elenco di malattie; offerte speciali, sconti, *kit* in omaggio.

Considerando i profili giuridici della questione, e dunque i poteri e le responsabilità del Garante, abbiamo avviato accertamenti su siti italiani, per verificare il rispetto di principi essenziali della protezione dei dati, come quelli riguardanti l'informativa a quanti richiedono il *test*, il consenso che gli stessi devono prestare, le modalità di comunicazione dei risultati, l'autorizzazione eventuale del Garante. Le questioni del consenso diventano particolarmente gravi per i *test* di

paternità, ordinariamente chiesti dal padre dubbioso utilizzando materiale genetico di un minore all'insaputa della madre, con conseguenze gravi sulla disciplina delle relazioni familiari.

Per quanto riguarda la comunicazione dei risultati, essendo la loro interpretazione particolarmente complessa nel caso dei *test* predittivi, e tale da poter incidere drammaticamente su scelte di vita, assume specifica rilevanza il secondo comma dell'art. 23 della legge n. 675 del 1996, che impone la comunicazione dei dati sulla salute tramite un medico di fiducia. Intermediazione peraltro insufficiente in questi casi, tanto che l'art. 12 della Convenzione europea di biomedicina condiziona la legittimità dei *test* predittivi ad "una consulenza genetica appropriata", ovviamente riferita all'intero processo, e non solo alla comunicazione del risultato finale. Poiché la Convenzione è stata ratificata con la legge n. 145 del 28 marzo 2001, sollecitiamo il Governo a depositare i relativi strumenti, permettendo così l'entrata in vigore di una normativa che, in particolare nella materia della genetica, può assicurare pienezza di tutela alla libertà esistenziale ed al diritto fondamentale alla salute.

La localizzazione delle persone e i "guinzagli elettronici"

Se il corpo investigato attraverso l'intima sua struttura genetica apre inquietanti prospettive, preoccupazioni nuove nascono dal diffondersi delle tecniche di localizzazione delle persone. Ormai consolidate attraverso i servizi di telecomunicazione, ed offerte dai loro gestori, queste tecniche cominciano ad utilizzare anche strumenti diversi, in particolare i *chip* che possono essere inseriti in qualsiasi prodotto e, come si è già ricordato, addirittura nel corpo umano. Esse individuano una dimensione nuova della sorveglianza, resa possibile dal mutamento sociale che ha portato il telefono mobile a divenire quasi una protesi della persona, un robustissimo e invisibile filo elettronico che permette di seguire ogni nostro movimento

in qualsiasi labirinto. A questo si accompagna l'interesse di un mondo imprenditoriale che vuole seguire la circolazione dei prodotti e, attraverso questa, ricostruire anche i comportamenti di acquirenti e utilizzatori.

Avevamo tra i primi segnalato il diffondersi della videosorveglianza, sulla quale continueremo a vigilare viste le molte utilizzazioni improprie da parte dei comuni. Ma le nuove forme di controllo capillare non sono più limitate agli spazi pubblici, ci seguono implacabilmente anche nei luoghi più intimi, neppure la casa offre più un riparo.

Il tema della localizzazione e della continua "tracciabilità" delle persone individua così una dimensione nella quale la protezione dei dati può intrecciarsi con quella di altri diritti fondamentali, inviolabili e indisponibili. Questo vuol dire che neppure il consenso dell'interessato può rendere legittimo l'inserimento nel suo corpo di un *chip* che permetta di seguirne i movimenti, o il ricorso a *chip* che, inseriti in un prodotto, rendano poi possibile il controllo dei comportamenti di chi lo utilizza. Il "guinzaglio elettronico" confligge con la dignità della persona.

La localizzazione attraverso il telefono esige valutazioni che muovano dagli stessi principi. Esclusa ogni utilizzazione lesiva della dignità o che indebitamente interferisca nell'altrui sfera privata, e ferme restando le regole sul consenso, si deve sottolineare che è stato riconosciuto il diritto a non essere localizzato, che consente di sottrarsi ad una opprimente forma di controllo sociale, senza stigmatizzazioni o discriminazioni nei confronti di chi concretamente esercita questo nuovo diritto.

Inoltre, ogni conservazione dei dati di traffico per un determinato periodo, che implichi anche la possibilità di ricostruire i movimenti della persona, deve essere adeguatamente motivata e circoscritta nel tempo, con riferimenti dettagliati ad eventuali situazioni di emergenza o esigenze di sicurezza. Viene così confermata la necessità, sottolineata con particolare forza nella Relazione dell'anno scorso, di

circoscrivere rigorosamente tempi e modalità di conservazione dei dati di traffico, in via generale, anche al di là dello specifico profilo della localizzazione.

La questione rimane aperta e, anzi, si è complicata dopo le richieste di estendere l'obbligo di conservazione anche ai dati riguardanti *Internet*. E qui i dubbi si fanno ancor più consistenti, poiché vengono in gioco non solo la libertà di "navigare" in rete, e dunque la versione nuova ed elettronica della libertà di circolazione, ma pure la libertà di manifestazione del pensiero e quella di associazione, vista la crescente vocazione di *Internet* ad essere proprio strumento di espressione e di organizzazione per milioni di persone.

Il Garante e i cittadini

Affrontando problemi nuovi, il Garante sente più forte la responsabilità istituzionale di "curare la conoscenza tra il pubblico delle norme che regolano la materia". Questo ha richiesto una strategia complessa, delineata nelle passate relazioni e che ha preso le mosse da un ripensamento della nostra struttura. Ora la riorganizzazione interna è compiuta, e possiamo misurarne gli effetti in termini di efficienza, grazie anche alla nomina di un direttore di gestione.

I dati statistici per il 2002 mostrano un incremento costante del lavoro dell'Ufficio rispetto al 2001. È raddoppiato il numero dei ricorsi definiti (da 211 a 500), gli interventi su segnalazioni e reclami sono passati da 2327 a 3689. Sono stati 12.800 le richieste di informazioni e i quesiti telefonici, ai quali si devono aggiungere 6.400 casi di assistenza telefonica alle notificazioni. Rimane statisticamente esiguo il numero delle impugnazioni dei nostri atti e provvedimenti: un risultato nel quale non si riflette una sorta di accettazione passiva della giurisprudenza del Garante, quanto piuttosto un dialogo persuasivo con tutti i nostri interlocutori.

Considerando ricorsi, reclami, quesiti e segnalazioni si giunge ad una cifra di 28.475, che conferma i dati degli anni precedenti per quanto riguarda i flussi verso il Garante, mettendo a dura prova l'intera struttura. Non è mancato l'impegno del personale in un lavoro che esige anche una capacità costante di tenere il passo di una opinione pubblica esigente e di una realtà tecnologica e sociale straordinariamente dinamica. Un ringraziamento per tutti, in particolare per la guida che all'intera attività è venuta dal Segretario generale.

Dobbiamo certo rafforzare la nostra capacità di risposta alle domande dei cittadini, rendendoli anche consapevoli dei poteri che possono direttamente esercitare. La ristrutturazione del nostro sito, la distribuzione in centinaia di migliaia di copie di piccoli opuscoli informativi dovrebbero favorire questo risultato. Speriamo che un buon risultato informativo sia venuto dallo *spot* diffuso sulle reti televisive e radiofoniche Rai: una novità nel mondo delle autorità indipendenti, resa possibile dalla collaborazione della Presidenza del Consiglio. Lo *spot*, è bene sottolinearlo, è stato prodotto direttamente da noi, a bassissimo costo, grazie alla generosità (nessuno ha richiesto compensi) di tutti i partecipanti a questa impresa.

In un solo punto non si registrano novità: il permanere di una straordinaria compattezza nel lavoro del collegio. Che non significa assenza di discussione, e persino di contrasti. Ma questo avviene in un clima di confronto così intenso che non può, poi, destar meraviglia l'unanimità che ha sempre accompagnato le nostre decisioni, risultato di un lavoro unitario e convergente. Merito, forse, anche delle particolari modalità di nomina del Garante.

A Parlamento e Governo deve essere indirizzata un'altra segnalazione. Abbiamo rispettato le decisioni della legge finanziaria sulla riduzione degli stanziamenti e quelle relative al taglio delle spese. Ma il mantenimento dei livelli qualitativi e quantitativi, che hanno finora caratterizzato l'attività del Garante, così come la capacità di orientamento culturale nelle infinite materie a noi affidate e la forte

iniziativa in campo internazionale, sarebbero sicuramente pregiudicati da una distribuzione delle risorse che privilegi criteri astratti, e non si fondi, invece, su di una puntuale valutazione delle esigenze di ciascuna istituzione.

Larghissimo, infatti, è lo spettro delle competenze del Garante e, probabilmente, la miglior politica informativa è quella che si concreta nella tempestiva risposta a domande diffuse nella società. Abbiamo constatato l'attenzione dei cittadini quando ci siamo occupati delle centrali rischi private, che coinvolgono interessi di milioni di persone. Ma, insieme alla capacità di intervenire a tutela di interessi di larga rilevanza sociale, è essenziale la prontezza nell'affrontare le questioni nuove. Accade da mesi nella materia dello *spamming*. Cogliendo le inquietudini suscitate dall'arrivo sul mercato dei nuovi telefoni cellulari in grado di inviare foto, gli *Mms*, abbiamo subito indicato le condizioni per il corretto uso di questa tecnologia.

Ma è l'intero sistema delle telecomunicazioni a costituire un vero nervo scoperto. Se i cittadini sono avidi di cogliere le opportunità che continuamente offre, sono pure particolarmente reattivi e chiedono tutela contro ogni utilizzazione impropria dei dati, contro ogni ostacolo opposto alle loro richieste di controllo dei diversi fornitori di servizi. Dopo essere intervenuto, insieme all'Autorità per le telecomunicazioni, per far sì che i nuovi elenchi telefonici consentano a ciascun abbonato di decidere liberamente se e come comparire in essi, il Garante sta rispondendo all'insieme delle questioni emerse in questo settore con provvedimenti che, oltre a quello già ricordato sugli *Mms*, hanno già riguardato l'invio di *Sms* da parte di soggetti istituzionali, ai quali si aggiungeranno nei prossimi giorni quelli riguardanti in generale gli *Sms* e la fatturazione dettagliata.

L'altra lunga frontiera, dove il Garante incontra l'opinione pubblica, è quella del sistema dell'informazione. Le richieste sono numerose, i nostri interventi sono particolarmente attenti alla tutela dei minori, al rispetto della dignità di tutti. Lo

sforzo è anche quello di promuovere una cultura comune attraverso un dialogo continuo con i giornalisti, anche attraverso attività formative, e affrontando i nuovi problemi legati all'informazione attraverso *Internet* e la telefonia cellulare.

Nell'ambito delle attività economiche assume rilievo particolare il trasferimento dei dati fuori dell'Unione europea, che coinvolge sia l'interesse delle imprese alla fluidità della circolazione delle informazioni, sia il diritto dei cittadini a mantenere intatte le loro garanzie. Stiamo attentamente seguendo le modalità di tali trasferimenti, ed abbiamo anche svolto una indagine conoscitiva su un campione delle 50 maggiori società italiane. Ha finora risposto l'80.8% degli interpellati. L'85.7% delle società effettua trasferimenti fuori dell'Unione europea, ricorrendo nella grande maggioranza dei casi al consenso degli interessati (83.3%). Poiché nelle risposte viene indicato anche il contemporaneo ricorso ad una molteplicità di strumenti, si registra un riferimento all'esecuzione di obblighi contrattuali nel 50% dei casi, una significativa utilizzazione dell'accordo *Safe Harbor* per i trasferimenti negli Stati Uniti (16.7%), un avvio promettente delle clausole contrattuali *standard* predisposte dall'Unione europea (8.3%). I soggetti interessati sono soprattutto gruppi societari. Analizzando il tipo di dati trasferiti, nella maggior parte dei casi si tratta di informazioni relative ai dipendenti, anche se sono rilevanti pure i trasferimenti relativi ai dati di altre società (clienti, concorrenti, fornitori). Il riferimento prevalente al consenso rivela una preferenza per gli strumenti più collaudati, ma esige pure una attenta verifica sull'effettivo rispetto di tutte le condizioni che legittimano il trasferimento.

Le garanzie, infatti, potrebbero apparire deboli se non venissero accompagnate da una adeguata attività di controllo. Per questo è stata rafforzata l'attività di ispezione, grazie anche ad un protocollo d'intesa con la Guardia di Finanza, il cui Comandante Generale intendiamo qui pubblicamente ringraziare. L'applicazione delle sanzioni, anche nei confronti di una pubblica amministrazione troppe volte distratta, rende più incisiva la nostra azione, e quindi il rispetto di regole scritte nell'esclusivo interesse dei cittadini.

La legittimazione sociale del Garante è affidata anche ad una sua percezione da parte dell'opinione pubblica come istituzione capace di tenere vivo un dialogo continuo con l'intera collettività, che da essa attende una capacità di regolazione in grado di assicurare sintonia tra sistema giuridico e dinamiche tecnologiche e sociali. In questa direzione assumono particolare rilievo i codici di deontologia e buona condotta, che ampliano responsabilità e poteri del Garante in settori delicatissimi come la disciplina di *Internet* e del rapporto di lavoro, della videosorveglianza e del *direct marketing*. Siamo di fronte ad un significativo mutamento del sistema delle fonti che, nell'ambito di una legislazione per principi, affida al Garante il compito di promuovere e governare un sistema flessibile di regole, omeostatico, per certi versi sperimentale, capace di quei rapidi aggiustamenti di fronte ad una realtà mutata che non possono essere richiesti agli interventi parlamentari.

I codici deontologici si inseriscono nel nuovo quadro istituzionale delineato dal testo unico ("codice") appena approvato dal Consiglio dei ministri sulla base dell'eccellente lavoro svolto dalla Commissione nominata dal ministro per la Funzione Pubblica. Si tratta del primo tentativo a livello europeo (e non solo) di codificare la complessa e dispersa materia della tutela dei dati personali. Ci accingiamo ad esprimere il nostro parere su questo testo e ci auguriamo che dai pareri delle Camere venga un ulteriore contributo alla migliore definizione della disciplina.

Mutamenti sociali e ragioni della libertà

Ma non si può fare buona politica di tutela dei dati personali in un paese solo. Bisogna partire almeno dal modello europeo, oggi rudemente messo alla prova da richieste come quella proveniente dall'amministrazione americana di poter disporre di una cospicua massa di dati su chi vola dall'Europa verso gli Stati Uniti, senza tener conto delle garanzie previste dalle norme europee e nazionali. Di fronte ad una posi-

zione della Commissione a dir poco arrendevole, ed alla passività di altre autorità nazionali, il Garante italiano ed il Gruppo dei garanti europei si sono rivolti ai vertici delle istituzioni dell'Unione, trovando una significativa risposta nel Parlamento europeo, che con un voto quasi unanime ha censurato l'operato della Commissione.

Se la partita è ancora aperta, lo si deve dunque ad una nostra iniziativa che ha preso sul serio i diritti riconosciuti dalla Carta, dalle direttive europee e dalle leggi interne dei diversi paesi. Questo atteggiamento di fermezza sui principi dovrebbe ora esser fatto valere dall'Unione europea anche a proposito del *Total Information Awareness Program* (Programma per la conoscenza totale delle informazioni), che l'amministrazione statunitense intende utilizzare per il controllo di tutte le comunicazioni di ogni cittadino del pianeta, eccezion fatta per gli americani. È in corso un confronto tra diversi modelli di tutela delle libertà, con molte istituzioni e personalità degli Stati Uniti attentissime al modello europeo. Il dialogo può essere fecondo soprattutto se si ricorda che il modello europeo è stato costruito partendo da ingredienti importati dagli Stati Uniti, l'idea moderna di *privacy* e le autorità indipendenti.

La libertà è oggi sfidata da molte volontà e molte tecniche rivolte alla costruzione di una società della sorveglianza. Per sfuggire a questo rischio servono strategie istituzionali adeguate. Lo spazio virtuale dev'essere sottratto alla pura logica di mercato, a quella che è stata chiamata la "*disneyzzazione*", che nega la sua natura di spazio pubblico.

Ma anche lo spazio reale, i tradizionali luoghi pubblici – strade, piazze, parchi, stazioni, aeroporti – vengono sempre più sottoposti ad un controllo capillare, scrutati implacabilmente, segnando così il passaggio da una sorveglianza mirata ad una generalizzata. È la stessa logica che presiede alla conservazione per periodi sempre più lunghi di tutti i dati riguardanti il traffico telefonico, la posta elettronica, la navigazione su *Internet*.

Il mutamento sociale è proprio qui. La sorveglianza si trasferisce dall'eccezionale al quotidiano, dalle classi "pericolose" alla generalità delle persone. La folla non è più solitaria e anonima. La digitalizzazione delle immagini, le tecniche di riconoscimento facciale consentono di estrarre il singolo dalla massa, di individuarlo e di seguirlo. Il *data mining*, l'incessante ricerca di informazioni sui comportamenti di ciascuno, genera una produzione continua di "profili" individuali, familiari, di gruppo. La sorveglianza non conosce confini.

Questa inarrestabile pubblicizzazione degli spazi privati, questa continua esposizione a sguardi ignoti e indesiderati, incide sui comportamenti individuali e sociali. Sapersi scrutati riduce la spontaneità e la libertà. Riducendosi gli spazi liberi dal controllo, si è spinti a chiudersi in casa, e a difendere sempre più ferocemente quest'ultimo spazio privato, peraltro sempre meno al riparo da tecniche di sorveglianza sempre più sofisticate. Ma se libertà e spontaneità saranno confinate nei nostri spazi rigorosamente privati, saremo portati a considerare lontano e ostile tutto quel che sta nel mondo esterno. Qui può essere il germe di nuovi conflitti, e dunque di una permanente e più radicale insicurezza, che contraddice il più forte argomento addotto per legittimare la sorveglianza, appunto la sua vocazione a produrre sicurezza.

Cercando di intrecciare i diversi fili che compongono la trama complessa della protezione dei dati, emerge con chiarezza sempre maggiore che molti problemi possono essere risolti solo in una dimensione che superi quella degli Stati nazionali. L'esperienza europea ci dice che questo è possibile, e ci offre strumenti e modelli in questo senso. Ma non basta. I casi dell'offerta dei *test* genetici, dello *spamming*, dell'intera gamma delle attività svolte su *Internet* ci rinviano ad una dimensione ben più larga, che tende a coincidere con quella planetaria.

Già nella Conferenza mondiale sulla *privacy* tenuta a Venezia nel 2000, il Garante italiano propose una Convenzione internazionale. Oggi la necessità di

questo strumento è sempre più avvertita. Sarebbe buona cosa se il Governo italiano cominciasse a muoversi lungo questa strada, facendo una sua proposta in occasione del semestre di presidenza dell'Unione europea.

Arrivare a questo tipo di documento richiede lunghe negoziazioni tra i governi. Ma l'avvio di una trattativa potrebbe stimolare tutti i soggetti coinvolti nella gestione di *Internet* (cittadini, *provider*, produttori, imprese, autorità garanti) a sperimentare codici comuni di autoregolamentazione, a verificare quali problemi possano essere risolti con strumenti tecnologici (*privacy enhancing techologies*), definendo così sperimentalmente il campo della futura Convenzione. Se non si arriverà a questa "costituzione di *Internet*", le regole rischieranno d'essere dettate soprattutto dalle logiche tecnologiche e dalle logiche (e dalle censure) di mercato.

Per quel che possiamo, intendiamo restare fedeli a un mandato che ci vuole modesti, ma determinati, custodi dell'eguaglianza e della libertà dei contemporanei.