GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

# Relazione 2003

Discorso del Presidente **Stefano Rodotà**

www.garanteprivacy.it

Signor Presidente della Repubblica,

un anno, quello passato, in cui la corsa delle tecnologie si è fatta ancor più impetuosa, ma pure l'anno in cui Governo e Parlamento hanno messo a punto il Codice in materia di protezione dei dati personali, poi entrato in vigore il 1° gennaio 2004, che contiene strumenti che assicurano proprio l'adeguamento della disciplina giuridica ad una realtà perennemente mobile.

Il Codice, infatti, ha un impianto nel quale assume specifica rilevanza la trama dei principi, da adattare poi alla molteplicità delle situazioni concrete. Irrobustisce il sistema della protezione dei dati personali, ormai solidamente collocata nel quadro dei diritti fondamentali. Fa così crescere le garanzie per la libertà delle persone. Rappresenta il primo esempio, su scala internazionale, di riordino generale di una materia complessa e mutevole.

## Un nuovo quadro di principi

L'innovazione sul piano dei principi si coglie fin dal primo articolo del Codice, che riproduce il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea (ora presente anche nell'articolo 50 del Progetto di Trattato che istituisce una Costituzione per l'Europa): "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Il trasferimento di questa norma nel sistema italiano rende non più proponibili interpretazioni riduttive della protezione dei dati personali, e stabilisce un legame solido tra ordinamento italiano e ordinamento europeo. E il legislatore ha voluto ulteriormente ribadire la sua volontà di considerare la protezione dei dati come un diritto fondamentale, nominandola esplicitamente nell'articolo 2 del Codice.

È stata così fatta una scelta impegnativa, che richiede coerenza. Le norme sulla protezione dei dati personali non sono certo incise sul bronzo, ma neppure possono essere considerate come pezzi di una leggina che può essere smontata appena i portatori di un interesse settoriale alzano la voce o al semplice annuncio di una possibile emergenza. Il Codice segna il passaggio da una situazione di frammentazione legislativa ad un sistema unitario. Ha dato vita ad un quadro di riferimento di medio periodo, che consente di seguire il cambiamento, ma al tempo stesso vuole offrire certezze. Se dovesse farsi strada la sensazione che si tratta di un testo manipolabile sotto la spinta dell'emozione o del piccolo interesse, diverrebbero labili le garanzie per i cittadini, sarebbero incentivati i comportamenti volti ad aggirare il Codice, verrebbero scoraggiate le iniziative volte ad adeguare alla nuova disciplina le strutture pubbliche e private, che esigono investimenti e non possono, quindi, essere assoggettate ad un regime di precarietà.

Inoltre, proprio perché ci troviamo in presenza di diritti fondamentali, non sono ammissibili cedimenti a logiche localistiche. Il Garante seguirà con attenzione la legislazione regionale, per evitare che venga incrinato il principio della parità di trattamento dei cittadini, indipendentemente dal luogo in cui si trovino a vivere.

Di tutto questo bisogna esser consapevoli perché il Codice è parte essenziale di un progetto più complessivo, fondato su riferimenti nazionali e sopranazionali, affidato anche ad una molteplicità di codici di deontologia e buona condotta che sviluppano i suoi principi in specifici settori. Questo è già avvenuto per l'attività giornalistica, la ricerca storica, la ricerca nell'ambito del sistema statistico nazionale. Si sono appena conclusi i lavori dei codici dedicati alle centrali rischi private ed al trattamento di dati statistici da parte di soggetti che non fanno parte del Sistan. Presto vedranno la luce i codici dedicati alle indagini investigative ed alla videosorveglianza, ai quali altri se ne aggiungeranno nel corso dell'anno, in particolare quelli

riguardanti Internet, i rapporti di lavoro, il *direct marketing*. Il nostro paese, dunque, si sta dotando di un significativo *corpus* legislativo sui rapporti tra l'organizzazione sociale e l'innovazione scientifica e tecnologica, terreno sul quale si misura ormai la capacità innovativa dei sistemi giuridici.

Proprio per rafforzare la trama dei principi, al fondamentale principio di dignità, e ai ben noti principi di finalità, pertinenza e proporzionalità si affiancano ora quelli di "semplificazione, armonizzazione ed efficacia" (art. 2.2 Codice) e di "necessità" (art. 3 Codice). Quest'ultimo merita una sottolineatura particolare. L'articolo 3 stabilisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

Si enuncia così una linea di politica del diritto particolarmente impegnativa, che mette anche in guardia contro pericolose derive tecnologiche. Si tratta di una indicazione importante, perché la protezione dei dati rischia ogni giorno d'essere compressa dalla crescente offerta sul mercato di tecnologie che rendono più agevole forme generalizzate di raccolta delle informazioni. Il principio di necessità diviene così un ineludibile *test* legislativo per valutare la legittimità delle raccolte di informazioni personali.

In ciò non è difficile scorgere la volontà di misurare l'accettabilità sociale e politica delle tecnologie anche dal punto di vista del rapporto tra mezzi e fini in una società democratica, come, peraltro, prescrive l'art. 8 della Convenzione europea dei diritti dell'uomo (1950), dove si subordina la possibilità di limitare la protezione della vita privata e familiare solo attraverso misure coerenti con il carattere "democratico" di una società. Il Codice rafforza il legame tra *privacy* e democrazia.

## Il ricorso alle tecnologie e gli "allarmi" del Garante

Abbiamo ricordato, in passato, che non tutto ciò che è tecnologicamente possibile è anche socialmente desiderabile, eticamente accettabile, giuridicamente legittimo. Oggi dobbiamo aggiungere che le derive tecnologiche possono produrre gravi effetti distorsivi. Distorsioni nell'uso delle risorse quando, ad esempio, queste vengono investite in impianti di videosorveglianza privi di vera utilità per la sicurezza. Distorsioni nell'organizzazione degli interventi quando, ad esempio, ci si affida a grandi banche dati centralizzate, tecnicamente difficili da gestire, vulnerabili agli attacchi, accompagnate da affidamenti in *outsourcing* spesso inadeguati, soprattutto tali da distogliere l'attenzione dalla necessità di raccolte e di indagini mirate. Distorsioni nella percezione e nell'analisi della realtà quando, ad esempio, le raccolte di informazioni vengono adoperate per frettolose traduzioni di un fenomeno in termini di ordine pubblico, invece di indagarne le ragioni sociali e di avviare, quindi, politiche più adeguate.

Le regole di *privacy* divengono così anche fattore di efficienza, e si rivelano strumenti indispensabili per una analisi dei rapporti tra società e tecnologia. Una valutazione d'"impatto *privacy*" dovrebbe ormai accompagnare molti interventi legislativi ed organizzativi. Altrimenti, la corsa verso raccolte sempre più imponenti di dati personali non produce strumenti migliori di conoscenza della realtà, ma un assordante "rumore di fondo tecnologico" che può addirittura rendere più complessa l'azione pubblica. L'affidarsi cieco alle tecnologie, ritenendo che in esse risieda ormai la soluzione di ogni problema, può risolversi in una delega in bianco, con la politica che rischia di farsi espropriare dei suoi compiti di scelta e di decisione su gravi questioni sociali.

Il Garante, fin dalle sue prime relazioni, ha sempre indicato casi concreti in cui

i rapporti tra società e innovazioni scientifiche e tecnologiche si presentavano in forme particolarmente critiche. Sono quelli che, nelle cronache giornalistiche, vengono definiti gli "allarmi" del Garante. E che allarmi sono davvero, nel senso che non si tratta di grida senza fondamento, ma di segnalazioni precoci di dinamiche che, poi, rivelano tutta la loro portata. Videosorveglianza, conservazione di enormi volumi di traffico telefonico, rilevanza dei dati genetici, *spamming*, controlli capillari sulle persone: questi sono alcuni dei temi sui quali negli anni passati abbiamo richiamato l'attenzione e che, poi, si sono rivelati fenomeni socialmente pervasivi, con problemi ineludibili a livello interno ed internazionale.

Questo lavoro prospettico rimane essenziale, non solo per attrezzarsi a fronteggiare il futuro, ma anche per non cadere nella *routine* burocratica. Ma non sappiamo fino a quando il Garante potrà tener fede a questo impegno se continuerà la lenta riduzione delle sue risorse. Questo stillicidio non pregiudica soltanto l'efficienza: rischia di minare la nostra autonomia. Raccogliendo una indicazione contenuta nella relazione dell'anno scorso, la Camera dei deputati ha votato all'unanimità una mozione nella quale si sottolinea appunto la necessità di attribuire al Garante le risorse necessarie. Su questa base ci siamo rivolti al Governo e speriamo che, in attesa di una più attenta considerazione nella prossima legge finanziaria, alcuni interventi siano già possibili attingendo al fondo di riserva.

Il futuro è già tra noi – si usa dire. Per questo il Garante dedica la sua attenzione anche a novità apparentemente minori, ad innovazioni ancora d'incerta applicazione. Solo così, infatti, si può evitare d'essere colti in flagrante peccato di distrazione, intervenendo quando la forza delle cose rende più difficile regolare situazioni in parte già consolidate.

Il sistema delle telecomunicazioni è quello che più visibilmente incorpora il

futuro. Si trasforma, offre agli utenti grandi opportunità, ma crea anche nuove vulnerabilità individuali e sociali. Dopo aver adottato provvedimenti sui messaggi di posta elettronica non desiderati *(spamming)* e sui messaggini telefonici *(Sms)* promozionali, il Garante sta per intervenire in tre direzioni. Quella della televisione interattiva, dove il continuo flusso di informazioni dall'utente al fornitore del servizio può consentire controlli continui sulle abitudini delle persone, ricavandone profili personali e di gruppo ed esponendo i singoli al rischio di nuovi controlli, se viene consentito ad autorità pubbliche di accedere a questi dati. Quella delle videochiamate, che possono coinvolgere una molteplicità di soggetti e richiedono, quindi, regole precise sull'utilizzazione delle immagini. Quella, infine, di un rigoroso controllo del modo in cui i diritti dell'utente vengono rispettati nell'ambito della telefonia, dove riscontriamo inadempimenti riguardanti questioni alle quali i cittadini sono assai sensibili, come le chiamate di disturbo e l'identificazione della linea chiamante.

## Etichette "intelligenti" e controlli sulle persone

Un anno fa sottolineavamo i problemi nascenti da tecniche di localizzazione che rendono possibile un controllo continuo delle persone, creando una sorta di guinzaglio elettronico. Su questa strada non ci si è fermati e, anzi, la tecnologia delle radiofrequenze *(Rfid)* ha portato alla creazione di "etichette intelligenti" che, sostituendo i codici a barre, permetteranno di seguire i prodotti nei loro spostamenti, creando così le condizioni per controllare anche chi ha acquistato ed usa quel prodotto.

Molti impieghi della *Rfid* sono sicuramente utili e benefici: migliore gestione delle merci, possibilità di rintracciare l'origine di prodotti particolarmente delicati (come i medicinali), rapidità di operazioni commerciali (lettura istantanea dei prezzi

di tutti gli oggetti posti nel carrello di un supermercato). Se, tuttavia, le etichette intelligenti non vengono disattivate nel momento in cui il prodotto passa nelle mani dell'acquirente, diventa reale il rischio di una sorveglianza generalizzata di persone e comportamenti.

Ma lo stesso corpo può essere tecnologicamente modificato, predisposto per essere seguito e localizzato permanentemente. Braccialetti elettronici sono stati proposti anche per controllare i bambini sulle spiagge. Ora la possibilità di inserire sotto la pelle un *chip*, contenente ad esempio informazioni sulla salute o tale da permettere in ogni momento la localizzazione di persone rapite, di criminali pericolosi, di detenuti in libertà provvisoria o più semplicemente l'identificazione di una persona, ha indotto una società americana a lanciare il servizio *VeriChip* con lo slogan *"Get chipped"*. Questa società ha poi presentato il servizio *VeriPay*, consistente sempre in un *chip* sotto la pelle, che dovrebbe prendere il posto di una comune carta di credito, rendendo così più sicuri e veloci i pagamenti. Il controllo diventa poi ancora più agevole se ci si affida alle etichette intelligenti, adoperandole per contrassegnare non solo prodotti, ma anche esseri viventi: oggi gli animali di un gregge, come già accade, in prospettiva anche le persone.

Siamo ormai di fronte alla concreta possibilità di vere e proprie modificazioni del corpo. Se, ad esempio, si considera la possibile sostituzione del braccialetto elettronico con le tecnologie *Rfid* per controllare i detenuti in regime di semilibertà o le persone agli arresti domiciliari, non assistiamo ad un innocente passaggio da una tecnologia all'altra. Per quanto odioso possa essere, il braccialetto non modifica il corpo. Ma quando si inserisce un *chip* o si applica una etichetta intelligente, l'integrità del corpo è violata, la dignità lesa, sì che l'impianto dovrebbe essere ritenuto illegittimo anche se la persona interessata abbia dato il suo consenso.

Si tratta, dunque, di stabilire quando la *Rfid* possa essere adoperata per raccogliere informazioni personali. Poiché la nuova tecnologia è in fase di decollo, il Garante interverrà nelle prossime settimane precisando le condizioni per il suo legittimo uso. Ferma restando l'inammissibilità di applicazioni dirette sul corpo, tutti i soggetti ai quali vengono trasferiti prodotti così "etichettati" dovranno ricevere una informazione adeguata ed essere messi nella condizione di ottenere prodotti per i quali sia stata disattivata la *Rfid* o di procedere direttamente alla disattivazione.

## Tecniche biometriche e libertà del corpo

Se questi usi del corpo possono sembrarci meno vicini, e più controllabili, lo stesso non può dirsi per le tecniche biometriche. Per documenti di identificazione d'ogni tipo, dai passaporti alle semplici carte d'identità, si esige sempre più largamente che in essi siano inseriti dati biometrici, ritenuti indispensabili per assicurare la certezza dell'identificazione.

Si dà così rilevanza, in modo nuovo, al corpo, che diventa fonte diretta di informazioni, oggetto di un continuo *"data mining"*, davvero una miniera a cielo aperto dalla quale attingere dati ininterrottamente. Lo ripetiamo: il corpo in sé sta diventando una *password*. La fisicità prende il posto delle astratte parole chiave, sostituite da impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, *Dna*.

L'insistenza sui dati biometrici si è fatta particolarmente martellante per la loro associazione con le esigenze di sicurezza. Ma qui valgono le considerazioni sulle derive tecnologiche e sulla necessità di riferirsi sempre ai principi del Codice.

Il principio di necessità impone di accertare se la finalità perseguita non possa essere realizzata utilizzando dati che non coinvolgano il corpo. Il principio di proporzionalità esige una considerazione rigorosa della legittimità di raccolte generalizzate rispetto a raccolte mirate, di una conservazione centralizzata o decentrata dei dati raccolti. Il principio di dignità fa emergere la necessità di rispettare l'autonomia delle persone di fronte a particolari raccolte di dati (quelle riguardanti la salute, in primo luogo).

Non ci si può limitare ad una generica analisi costi-benefici. Quando si incide su libertà personale, integrità e dignità, non si può agire come se il bisogno di sicurezza o il fine dell'efficienza potessero prevalere su ogni altra considerazione. Difendendo la persona e il suo corpo si difendono valori fondamentali dei sistemi democratici, che non possono essere limitati o sacrificati senza avviare pericolose derive di tipo totalitario.

L'utilizzazione dei dati biometrici offre certamente nuove forme di sicurezza, semplificazioni delle attività quotidiane. Aumenta la certezza delle identificazioni e delle verifiche dell'identità. Può facilitare attività investigative.

Ma non ci si può limitare a registrare il contributo tecnico della biometria alle attività di identificazione e verifica. È indispensabile assicurarsi della loro accuratezza, poiché le tecniche utilizzate possono determinare percentuali elevate di falsi positivi e negativi. Questo accade per il carattere ancora sperimentale di alcune tecniche o dipende dalle particolari condizioni in cui vengono impiegate (come le condizioni di luce o l'angolo di ripresa per l'identificazione facciale).

Il ricorso ai dati biometrici, quindi, esige un approccio tecnicamente prudente, senza gli entusiasmi e le definitive certezze che spesso vengono proclamate soprat-

tutto da chi ha interesse  a collocare sul mercato le relative tecnologie. In un documento dell'Ocse del marzo di quest'anno *(Biometric-based Technologies)* si osserva che una rassegna delle informazioni disponibili dà "al lettore la sensazione che la biometria non sia ancora 'pronta per la prima serata'". Questo vuol dire che, mentre queste tecnologie sembrano funzionare adeguatamente in impieghi ridotti e limitati, "la loro accuratezza, affidabilità e adeguatezza non sono ancora sufficientemente raffinate per una loro utilizzazione in sistemi di identificazione personale su larga scala".

Da questo tipo di analisi si traggono due indicazioni. Una riguarda il periodo breve-medio, e consiglia una valutazione rigorosa dell'uso dei dati biometrici con riferimento alla loro affidabilità: si tratta, evidentemente, di indicazioni destinate a variare a seguito dei perfezionamenti tecnici. L'altra ha carattere generale e si riferisce al *test* di compatibilità con i valori di libertà e democrazia al quale anche le utilizzazioni dei dati biometrici devono essere sottoposte, secondo le indicazioni desumibili anche da un parere del Gruppo europeo dei garanti.

Si sono già ricordati i principi di necessità e proporzionalità, rilevanti anche per valutare la legittimità di raccolte di dati riferiti ad un gran numero di persone. Le raccolte generalizzate, infatti, soprattutto se giustificate genericamente con ragioni di sicurezza, modificano la percezione sociale di tali raccolte e trasformano tutti i cittadini in potenziali sospetti. Fanno crescere la vulnerabilità sociale, essendo difficile eliminare il rischio di abusi o difendere le grandi banche dati da violazioni operate anche da gruppi terroristici o criminali. Diversi studi propongono in modo persuasivo argomenti sull'inefficienza e sui limiti delle grandi raccolte d'informazioni.

Il ricorso massiccio alle soluzioni basate sulla biometria può essere presentato e percepito come una panacea tecnologica, sì che l'opinione pubblica tende a

sopravvalutare la loro accuratezza, associando impropriamente tali tecnologie con una protezione assoluta contro il terrorismo. A questa falsa certezza può associarsi una crescente "mitridatizzazione" sociale. Il diffondersi del ricorso alla biometria oltre le situazioni di stretta necessità rischia di far progressivamente perdere ai cittadini la sensibilità necessaria per avvertire i rischi per la loro libertà personale. La società può essere anestetizzata attraverso la progressiva cancellazione delle percezioni legate alla perdita del controllo esclusivo sul proprio corpo.

Cogliamo un'inquietudine sociale di fronte ad invasive forme di appropriazione del corpo attraverso i dati sulla salute. Possono farlo soggetti pubblici: per questo abbiamo segnalato l'improprietà e la pericolosità di raccolte centralizzate di dati sulla salute per finalità di controllo sulla spesa sanitaria e siamo intervenuti per evitare improprie comunicazioni sull'identità delle persone in materia di procreazione assistita. Possono farlo soggetti privati: per questo continuiamo a controllare l'offerta su Internet di *test* genetici, e in generale le questioni della genetica, alle quali ha recentemente dedicato un parere il Gruppo europeo dei garanti.

## Trasformazioni della persona

Davanti a noi sono mutamenti che toccano l'antropologia stessa delle persone. Siamo di fronte a slittamenti progressivi: dalla persona "scrutata" attraverso la videosorveglianza e le tecniche biometriche si può passare ad una persona "modificata" dall'inserimento di *chip* ed etichette "intelligenti", in un contesto che sempre più nettamente ci mostra come stiamo diventando *"networked persons"*, persone perennemente in rete, via via configurate in modo da emettere e ricevere impulsi che consentono di rintracciare e ricostruire movimenti, abitudini, contatti, modificando così senso e contenuti dell'autonomia delle persone.

I servizi di localizzazione si diffondono e si diversificano, utilizzando la telefonia cellulare, la tecnologia delle radiofrequenze, i sistemi di rilevazione satellitare (che diverranno più efficienti con l'entrata in funzione del sistema Galileo). La localizzazione può riguardare lo stesso interessato o soggetti terzi; può interessare aree vaste o luoghi circoscritti; può essere momentanea o protratta nel tempo; può fornire servizi che vanno dal controllo di veicoli allo spostamento di persone. Riflettendo sui loro diversi effetti, si può dire che le tecnologie elettroniche, dopo aver contribuito in modo essenziale all'annullamento della distanza e creato le condizioni per controlli capillari, stanno anche facendo riscoprire la "prossimità". Infatti, quando i servizi di localizzazione sono solo quelli richiesti dall'interessato e riguardano l'area in cui egli stesso si muove, mettono la persona nella condizione di valorizzare la vicinanza fisica con altre persone o con specifici servizi.

Il rimanere perennemente in rete, peraltro, può modificare, o cancellare del tutto, il "diritto all'oblio". Fino a ieri una notizia apparsa anni prima su un giornale locale, una vecchia foto pubblicata in un remoto gazzettino, non seguivano implacabilmente la persona alla quale si riferivano. Oggi è sufficiente che quella notizia o quella foto si riferiscano ad una persona appena nota, o abbiano fatto parte di una vicenda di qualche rilevanza, ed ecco che basta digitare un nome su un motore di ricerca per farle riaffiorare, rendendo estremamente difficile il ricorso agli strumenti che possono consentire ad una persona di non rimanere prigioniera di un passato che non passa. E lo stesso divieto d'indagine sulle opinioni dei lavoratori, importantissima conquista sancita dall'articolo 8 dello Statuto dei lavoratori, rischia d'essere aggirato da esplorazioni in rete che non lasciano traccia.

A questo mutamento non assistiamo passivamente, e di esso non parliamo soltanto perché possa aversene pubblica consapevolezza. Interventi del Garante italiano, del Gruppo europeo sulla protezione dei dati personali, di molte autorità nazionali indicano le strade di una concreta strategia.

Abbiamo appena approvato un nuovo, ampio provvedimento sulla videosorveglianza, dove si individuano i modi per combinare correttamente libertà delle persone, esigenze di controllo, efficienza amministrativa. Per quanto riguarda le impronte digitali, abbiamo stabilito condizioni rigorose per eventuali e limitati trattamenti da parte dei privati, opponendoci, ad esempio, ad una loro utilizzazione per il semplice controllo dell'accesso a mense universitarie; ed attendiamo la relazione del Governo al Parlamento, come previsto da una mozione approvata dalla Camera dei deputati, per quanto riguarda le modalità della loro raccolta generalizzata a fini di identificazione, sulle quali esprimeremo il nostro parere. Registriamo positivi contatti con il Dipartimento per la pubblica sicurezza del ministero dell'Interno in materia di impronte digitali sui permessi di soggiorno e per la distinzione tra impronte dei comuni cittadini e impronte di persone sospettate. Sui diversi progetti di costituzione di banche dati del *Dna* diciamo fin da ora che esse devono essere limitate a finalità di particolare rilevanza e specificamente individuate, devono riguardare categorie assai circoscritte di soggetti, devono raccogliere i soli dati rilevanti per l'identificazione (con esclusione, quindi, di tutto quel che ha valenza predittiva o consente di risalire ad altri soggetti), devono precisare i rapporti tra i dati raccolti ed il materiale genetico dal quale sono estratti. No, in ogni caso, a tutto ciò che si presenta come schedatura di massa o ad utilizzazioni anche solo potenzialmente discriminatorie. Né finalità di sicurezza, e tanto meno interessi economici, possono mettere in discussione l'ineludibile principio d'eguaglianza. Pure in un ambiente come quello degli Stati Uniti, dove la forza della *business community* è persino straripante, il Senato ha approvato all'unanimità un progetto di legge che vieta ogni utilizzazione dei dati genetici da parte di assicuratori e datori di lavoro *(Genetic Non-Discrimination Act)*.

Questa strategia, oltre a ribadire il rigoroso riferimento ai principi di necessità, finalità, pertinenza e proporzionalità, sottolinea la necessità di una precisa distinzione tra finalità di identificazione e di verifica. Manifesta una preferenza per i

sistemi decentrati rispetto a quelli centralizzati e per una identificazione su base strettamente individuale (1:1) piuttosto che facendo riferimento a banche dati contenenti informazioni su una molteplicità di soggetti (1:M). Diverse autorità di controllo europee, infatti, sostengono già che i dati biometrici non dovrebbero essere raccolti in banche dati centralizzate, ma inseriti in un oggetto nella disponibilità diretta dell'interessato, come una carta con *microchip*, un telefono cellulare, una carta di credito. L'identificazione e la verifica, in altri termini, dovrebbero essere effettuate comparando il dato contenuto in quell'oggetto con il dato fornito dall'interessato al momento dell'identificazione e/o della verifica.

## Libertà, sicurezza, diritti fondamentali

Si tratta di una strategia volta a mostrare l'improprietà delle tesi che vogliono identificare la tutela della sicurezza con la compressione della protezione dei dati personali, dunque di diritti fondamentali. Non solo sono possibili bilanciamenti tra i diversi interessi, ma è comunque indispensabile che ogni eventuale limitazione venga accompagnata da nuove garanzie, adeguate alla diversa situazione che si è creata. Un esempio può essere tratto proprio da una vicenda che ha comportato una modificazione dell'articolo 132 del Codice. Ritenendosi inadeguato il termine di trenta mesi per lo svolgimento delle indagini su reati particolarmente gravi, si è portato questo termine a quarantotto mesi. Ma questa "perdita" è stata, almeno in parte, "compensata" da modalità ancor più garantite di custodia "sotto chiave" dei dati, dalla riduzione a ventiquattro mesi del termine generale di conservazione, di cui si giovano tutti i cittadini, e dalla limitazione dell'utilizzabilità solo per una serie di reati gravi dei dati conservati per i successivi ventiquattro mesi.

Non siamo, evidentemente, insensibili ai temi della sicurezza. Ma operiamo

perché essi vengano affrontati in modo razionale, depurando le proposte dal tasso di emotività o improvvisazione che finiscono col renderle inefficienti, sottolineando sempre che il rispetto dei diritti e delle libertà fondamentali non è solo un dovere imposto dalle leggi, ma un formidabile "valore aggiunto" per la democrazia nella lotta contro chi, terroristi in primo luogo, negano con i loro atti proprio i suoi valori.

Lavoriamo per questo non soltanto in Italia. Un virtuoso circuito istituzionale ha ben funzionato nell'Unione europea. Infatti, solo grazie all'azione congiunta del Parlamento europeo e del Gruppo europeo dei garanti è stato finora possibile porre un argine alla pretesa dell'amministrazione americana di ottenere praticamente senza condizioni decine di milioni di dati sui passeggeri delle linee aeree in viaggio verso gli Stati Uniti, mentre altri paesi, come l'Australia e il Canada, hanno accettato le richieste di garanzie avanzate dall'Unione europea. Lo abbiamo detto in passato, e lo ripetiamo oggi: non si tratta di una vicenda circoscritta, ma di un confronto tra modelli di tutela dei diritti. E la sensibilità per il diritto e per i diritti, che la vecchia Europa continua a dimostrare, si conferma come una riserva di saggezza per tutti.

Per questo, dopo aver mostrato ieri che attraverso la protezione dei dati personali si giunge ad una vera "costituzionalizzazione della persona", richiamiamo oggi l'attenzione sulla necessità di una rilettura di molti tradizionali diritti. Il costante riferimento alla necessità di "rispetto dei diritti e delle libertà fondamentali" (art. 2.1 Codice) non implica soltanto un confronto concreto tra le specifiche forme di trattamento dei dati personali e i singoli diritti e libertà. Impone ormai una ricostruzione di libertà e diritti aderente all'ambiente tecnologico nel quale vengono esercitati: dalla considerazione come "formazioni sociali" delle comunità virtuali alla libertà di circolazione in luoghi videosorvegliati, dalla segretezza delle comunicazioni in Internet all'estensione della promessa della *Magna Charta* – "non metteremo mano su di te" – dal corpo fisico al corpo elettronico.

Consapevoli di tutto questo, abbiamo ritenuto che molte proposte di conservazione dei dati di traffico su Internet siano in conflitto con la dimensione dei diritti fondamentali. Ma non abbiamo mai considerato la rete come uno spazio senza regole. Basta ricordare i nostri interventi in materia di *spamming*, che hanno preso le mosse proprio dalla considerazione che la semplice reperibilità su Internet di un indirizzo di posta elettronica non implica la sua libera appropriabilità da parte di chiunque. In questo senso, il recente provvedimento in materia di propaganda elettorale, oltre a costituire un *vademecum* per i candidati, contribuisce a chiarire la differenza tra i diversi strumenti – posta tradizionale, stampa, telefono, comunicazione elettronica. Quest'ultima crea uno spazio del tutto nuovo, dove i cittadini devono poter esercitare una duplice libertà: quella d'essere al riparo da ogni comunicazione indesiderata e quella di potersi esprimere liberamente, nella forma della comunicazione e del collegamento. Questo spazio di libertà, non comparabile a quello individuato dagli altri mezzi di comunicazione e dove già si scambiano ogni giorno 300 milioni di messaggi elettronici, esige un grado di tutela particolarmente intenso.

## Garante, istituzioni, cittadini

Il Codice ha aperto al Garante nuove possibilità di azione con l'articolo 154, estendendo il suo potere di segnalazione anche al Parlamento, e non più al solo Governo. Nasce così un nuovo circuito istituzionale, che si spera virtuoso quanto quello europeo.

Questo potere è già stato esercitato, in particolare nelle delicatissime materie della tutela dei dati sulla salute e della conservazione dei dati del traffico in rete. Da qui ha preso le mosse una collaborazione complessivamente assai positiva, testimo-

niata anche da alcuni voti unanimi con i quali la Camera dei deputati ha assunto posizioni che sottolineano l'importanza della tutela di questa nuova dimensione della libertà.

Il legame con il Parlamento, peraltro, riflette la specifica legittimazione del Garante, che vede i suoi quattro componenti scelti da un voto delle Camere. E il rafforzamento del Garante è in linea con l'emersione sempre più netta della sua natura di istituzione di garanzia, confermata anche dalla Carta dei diritti fondamentali dell'Unione europea e dal Progetto di Trattato per una Costituzione europea. Solo per i dati personali, infatti, è qui prevista la necessaria presenza di una autorità indipendente, che assume così una rilevanza "costituzionale". Per queste ragioni, perdurando la discussione sulla riforma delle autorità indipendenti, siamo dell'opinione che sarebbe preferibile il mantenimento delle attuali modalità di nomina dell'intero collegio che, proprio perché affidate al Parlamento, ne garantiscono meglio l'indipendenza. Lo ricordiamo anche perché davanti alla Commissione europea è stato sollevato un dubbio sulle modalità di nomina di alcune autorità europee, con l'argomento che il peso esercitato dall'esecutivo farebbe venir meno i requisiti di indipendenza richiesti della Direttiva 95/46.

L'azione del Garante non si esaurisce nei pur ricchi circuiti istituzionali interni ed internazionali. Vive sulla lunga frontiera del rapporto con il singolo cittadino, nel dialogo con l'opinione pubblica. Quello che oggi sta davanti a voi è un Garante più aperto e attento, non prigioniero di una banale logica di "comunicazione", ma consapevole della necessità di parlare e di essere compreso.

Prendendo sul serio il principio di semplificazione, è stato messo a punto un sistema di notificazioni elettroniche che non teme confronti con i sistemi degli altri paesi. Per gli obblighi di notificazione è stato delineato un percorso che offre più

ampi margini per adottare le misure di sicurezza. Abbiamo avviato una innovativa attività di formazione rivolta al mondo privato e a quello pubblico. Si svolgeranno nelle prossime settimane un seminario sullo *spamming* e un convegno sulle innovazioni tecnologiche. Con il codice di deontologia sulle centrali rischi private ci rivolgiamo ad una vastissima platea di cittadini, in un momento in cui il credito al consumo assume specifica rilevanza. Sono state rese più efficienti le strutture di rapporto con l'esterno. E tutti i componenti del Garante si sono recati in varie città, per illustrare direttamente i temi della protezione dei dati.

Segni, tutti, di una attenzione per le situazioni reali. Esattamente l'opposto di quella *"buroprivacy"* che qualcuno impugna come argomento contro il Codice e che, quando non è segno di cattiva coscienza, si traduce nella pretesa di annullare garanzie di tutti i cittadini per l'interesse magari di un gruppo ristretto.

Abbiamo reso più agevole la conoscenza e l'utilizzazione del nostro lavoro con le newsletter, e soprattutto con la pubblicazione di un Massimario riassuntivo di tutta la nostra "giurisprudenza", seguito con particolare attenzione dal nostro Vicepresidente, Giuseppe Santaniello. È imminente l'uscita di una raccolta di scritti su *privacy* e attività produttive, voluta da Gaetano Rasi. In un altro volume, "*Privacy* e giornalismo", Mauro Paissan ha sistemato i nostri interventi nel settore sensibilissimo dei mezzi di comunicazione. Senza mai cedere a tentazioni censorie, a paternalismi o a rigurgiti di moralismo, il Garante ha cercato di rendere effettiva una tutela di cui hanno bisogno, proprio per l'invadente spettacolarizzazione d'ogni momento della vita quotidiana, soprattutto i cittadini "comuni". E su questi temi è in corso un lavoro con l'Ordine dei giornalisti.

Sono aumentate le ispezioni, sono divenute più penetranti, hanno portato anche alla segnalazione all'autorità giudiziaria di ipotesi di reato. Rafforzeremo que-

sta attività, anche grazie all'eccellente collaborazione con la Guardia di finanza. Non sorprenda questo riferimento alle ispezioni, dunque ad un'attività repressiva, in una parte dedicata all'apertura all'esterno del Garante. Basta leggere le frequenti lettere ai giornali, per rendersi conto che nulla infastidisce i cittadini più dei casi in cui la legge sulla *privacy* è violata con intenzione, se non con protervia.

Ma, come sempre, sono le nude cifre ad avere la più forte eloquenza. Abbiamo deciso ben 775 ricorsi (erano stati 500 nel 2002), un impressionante dato quantitativo che rende immediatamente evidente una scelta preferenziale per la risoluzione delle controversie ad opera del Garante piuttosto che dall'autorità giudiziaria. Emerge così la più vera natura del Garante, quella di essere interlocutore diretto dei cittadini, come confermano le 4914 risposte a quesiti, segnalazioni e reclami (3689 nell'anno precedente) e, soprattutto, lo spettacolare balzo in avanti delle risposte a richieste di informazioni per telefono, passate da 12.800 a 38.000. In questi dati, più che il riflesso di difficoltà interpretative e applicative, riteniamo che debba scorgersi proprio l'effetto della migliore informazione sull'accesso al Garante e della riorganizzazione dell'Ufficio per le relazioni con il pubblico. Quale che sia la spiegazione più corretta di questo fenomeno, comunque, le cifre appena ricordate sono un segno di efficienza e, se scomposte nelle molteplici materie a cui si riferiscono, rivelano quanto sia larga l'area che la nostra attività deve coprire ogni giorno – salute, credito, telecomunicazioni, genetica, informazione, sicurezza, assicurazioni, pubblica amministrazione. Qui, in questo continuo confronto con il mondo, è il fascino del nostro lavoro.

Di fronte a tutti questi compiti, le forze di cui disponiamo sono inadeguate. Ma riusciamo a farcela lo stesso – tra mille difficoltà, e magari con qualche ritardo o conflitto. Per questo è grande il ringraziamento di tutto il Collegio, e il mio personale, a questa piccola e operosa comunità di lavoro, qui rappresentata dal segretario generale, Giovanni Buttarelli.

Vita privata e presenza pubblica

Lavorando così come facciamo, ci troviamo di fronte ad un altro problema. Spesso ai cittadini viene promesso un futuro pieno di efficienza amministrativa e occultato un presente in cui si moltiplicano gli strumenti di un controllo sempre più invasivo e capillare. Sembra quasi che si stiano costruendo due mondi non comunicanti, e che l'*e-government*, l'amministrazione elettronica, possa evolversi senza tener conto dei diritti individuali e collettivi. Noi proviamo a tenere insieme questi due aspetti, per restituire ai cittadini una immagine unitaria dell'ordinamento, così come ci preoccupiamo dell'unità della persona.

Si giunge così ad un altro punto di paragone, per noi ineludibile – quello del rapporto tra pubblico e privato. Una ventina d'anni fa, Albert Hirschman scriveva che "l'inversione verso la vita privata può essere considerata come un movimento verso la realtà, verso la sincerità, addirittura verso l'umiltà. Come la vita pubblica può consolarci della noia della vita privata, così la vita privata ci offre un riparo contro il parossismo e la futilità degli impegni pubblici". L'intimità come fattore di equilibrio, e dunque come possibilità di liberazione da altre tirannie.

A condizione, però, che non diventi disincanto, o distacco. Per ciò interpretiamo sempre più nettamente la protezione della vita privata non come un ritrarsi dalle brutture del mondo, non come un impossibile rifiuto del mutamento tecnologico, ma come una precondizione per l'esercizio pieno delle libertà e dei diritti. Lo diciamo ancora una volta: come un elemento prezioso della personalità e della cittadinanza.