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.