Relazione2003

Discorso del Presidente **Stefano Rodotà**

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