RELAZIONE PER L'ANNO 2005

Discorso del Presidente
Francesco Pizzetti

Roma, 7 luglio 2006

PAGINA BIANCA

Signor Presidente della Repubblica,

Signori Presidenti delle Camere,

Signore e Signori,

nel presentare per la prima volta la Relazione sull'attività dell'Autorità, i miei colleghi ed io sentiamo profondamente l'importanza dell'appuntamento e dell'eredità ricevuta dai componenti dei Collegi precedenti al nostro, presieduti dalla grande personalità di Stefano Rodotà. Collegi che hanno edificato e diffuso nel Paese la cultura della privacy, intesa come un più avanzato diritto fondamentale, a presidio della libertà e della dignità delle persone nella società dell'informatizzazione e del trattamento sempre più massiccio dei dati personali.

Il Garante ha dato vita in questi anni ad una significativa esperienza umana e professionale. Ha raccolto intorno a sé donne e uomini di valore che, insieme al Segretario Generale, hanno maturato competenze e professionalità e che vanno ringraziati per il grande impegno profuso.

A livello europeo, l'Autorità ha assunto un ruolo trainante e, anche per il contributo personale di Rodotà, la tutela dei dati è oggi un diritto fondamentale dei cittadini europei, sancito nella Carta dei diritti dell'Unione e poi trasfuso nel Trattato costituzionale che prevede espressamente i Garanti della protezione dei dati personali, come le sole "necessarie" Autorità indipendenti.

Abbiamo ricevuto un patrimonio prezioso che intendiamo onorare, persuasi che, in una democrazia matura e rispettosa della dignità della persona, la protezione dei dati rappresenta un crocevia in cui si intersecano interessi, valori e diritti.

La protezione dei dati personali nelle società "a cambiamento velocissimo"

Le tecnologie si sviluppano con una rapidità inaudita; le relazioni fra gli uomini e i popoli hanno una dimensione globale e una latitudine in cui, senza la

mediazione della tecnica, l'orizzonte non è più visibile allo sguardo dell'uomo; il bisogno di comunicare, di raggiungere tutti e ognuno, convive con l'aspirazione ad un'esistenza sicura, posta al riparo da vecchi e nuovi pericoli.

La società della tecnica, già diventata nel secolo scorso una società "a cambiamento veloce", è divenuta oggi una società "a cambiamento velocissimo".

Il nostro bagaglio di cognizioni è sempre più inadeguato a dare risposte convincenti e persuasive agli interrogativi che gli sviluppi della tecnica pongono alla nostra coscienza.

Rispetto a questa incredibile metamorfosi, è naturale interrogarsi sulla possibilità dell'uomo di esercitare un ruolo di guida e di governo del progresso tecnico; sulla sua capacità di indirizzare l'uso della tecnologia, che è un mezzo, verso fini e risultati al servizio dell'uomo e rispettosi della sua dignità.

La tecnologia può essere un formidabile strumento di libertà oppure causa di inedite differenziazioni sociali.

È qui che si colloca il valore fondamentale racchiuso nelle regole e nei comportamenti in cui consiste il diritto alla privacy.

La protezione dei dati personali assolve un ruolo essenziale nella ricerca di un rapporto armonico e bilanciato fra l'uomo e la tecnica; fra la società in continuo divenire e la capacità di adattamento dell'individuo.

È indispensabile l'esistenza di istituzioni capaci di assicurare che i dati accumulati grazie alle tecnologie non siano usati *contro* di noi, ma solo *per* noi.

In una società libera e democratica, la tutela dei valori e dei principi connaturati all'essere cittadino rappresenta la risposta più efficace per contrastare una lettura pessimista del progresso.

La compatibilità democratica e l'accettazione sociale della tecnologia richiedono un sistema di garanzie che a pieno titolo comprende anche la protezione dati.

Più cresce la mobilità esistenziale e sociale che, consapevolmente o inconsapevolmente, ci fa disperdere parti del nostro essere in innumerevoli luoghi, più è

essenziale l'attività di un'Autorità che, proteggendo i dati di ciascuno da trattamenti indebiti, consenta di tenere l'identità di tutti al riparo da una frammentazione e ricomposizione artificiale, che trasformerebbe ciascuno di noi in una "cosa".

Opportunità e timori

La protezione dei dati personali si situa, dunque, sul confine che divide la fiducia dalla paura, l'oppressione e il controllo dalla libertà e dalla democrazia.

Solo se si è certi che vengono richieste le informazioni realmente necessarie, e che queste sono protette e rese inaccessibili a chi non ha diritto di conoscerle, si potranno sfruttare senza timore le opportunità che la tecnica offre.

Perché si deve temere che la carta di credito usata via Internet possa essere clonata o che la rilevazione della targa dell'auto possa essere usata per tracciare gli spostamenti e localizzare le persone?

Perché quando si fa una telefonata, si manda un *sms* o una *e-mail*, si accede a un sito Internet, si deve aver timore di essere ascoltati, letti, spiati?

Perché quando si acquista un prodotto si deve aver paura che vi sia chi analizza le nostre scelte per conoscere e profilare i gusti, le preferenze, la stessa capacità di acquisto?

Perché si deve essere costretti a guardare con timore alla richiesta di avere un dato biometrico e il DNA, anche quando questa richiesta sia fatta per curare o per proteggere?

Perché accettare che il grande villaggio globale debba essere una giungla senza regole, nella quale informazioni, errate o esatte, obsolete o recenti, possano essere catturate e diffuse senza che sia possibile verificare chi e per quali scopi lo fa, e senza che si possa rivendicare che esse siano rettificate o cancellate?

Perché dovremmo accettare di perdere la nostra anima per salvare il nostro corpo o, al contrario, rischiare di perdere il nostro corpo per salvare la nostra anima?

Sono dilemmi di fronte ai quali le nostre società non devono essere costrette a trovarsi. Mai!

La nostra Autorità, anche nell'anno trascorso, si è interrogata su tutto ciò. Abbiamo agito con l'obiettivo di governare, per quanto ci è possibile, il cambiamento in corso.

Nei settori maggiormente esposti, abbiamo intensificato le attività di disciplina, di verifica e di accertamento.

Tra i provvedimenti più innovativi possiamo ricordare quelli che hanno precisato i limiti e i casi in cui l'utilizzo dei dati biometrici può essere applicato ai lavoratori; il provvedimento generale di inizio d'anno sull'uso delle etichette intelligenti (o RFID) e le successive decisioni relative ai limiti della loro applicazione negli istituti bancari e nei luoghi di lavoro; l'iniziativa – la prima da parte di un'Autorità di protezione dati – assunta nei confronti di Google, al fine di ottenere che le regole della *privacy*, dalla rettifica dei dati sino al diritto all'oblìo, siano rispettate dai motori di ricerca in Internet, anche quando il gestore sia stabilito fuori del territorio italiano.

L'attività svolta con Google America, peraltro ancora in corso, assume una ulteriore valenza. Essa è un primo passo concreto per introdurre garanzie per gli utenti adeguate alle attuali forme di utilizzazione di Internet. Un passo che stiamo facendo anche con il sostegno delle altre Autorità europee.

Ci guida la consapevolezza che la mancanza di poteri regolatori sovranazionali e la perdurante assenza della tanto necessaria "Costituzione di Internet", se rappresentano un'espressione della libertà nella rete costituiscono però anche un serio limite ad un'effettiva tutela nel mondo telematico.

È la stessa consapevolezza che ci ha spinto a promuovere sul versante nazionale l'elaborazione di un codice deontologico degli operatori di Internet, che speriamo possa vedere la luce entro l'anno.

Le imprese e il lavoro nella rete dei dati

Anche il sistema economico è coinvolto in questo processo di innovazione, che moltiplica il trattamento dei dati.

Nonostante ciò, la tutela dei dati personali è spesso avvertita dal mondo delle attività produttive come un vincolo e un freno.

É probabile che questa opinione trovi giustificazione nella strumentazione giuridica, che in alcuni casi è generale ed uniforme e, quindi, non coglie a pieno le differenze fra le diverse realtà produttive e le diseguali dimensioni di impresa. Possono, pertanto, essere opportune idonee soluzioni di semplificazione.

Un punto però deve essere tenuto ben fermo.

La protezione dei dati personali non è un "lusso" o un "orpello" a cui possiamo rinunciare. È una necessità in un mondo in cui l'uso di dati è condizione vitale per la crescita economica e spesso per la sopravvivenza delle imprese.

Se il portafoglio ordini, i sistemi di approvvigionamento, i dati relativi ai dipendenti, ai consulenti, ai clienti, non sono protetti, può essere a rischio una parte essenziale del patrimonio aziendale, dell'avviamento commerciale, del valore stesso del marchio.

La protezione dei dati può e deve essere un "valore aggiunto".

Sui giornali campeggiano spesso inserzioni pubblicitarie che propongono l'acquisto di apparecchiature "sicure". Man mano che crescerà la consapevolezza dei valori e dei pericoli in gioco, vedremo sempre più le imprese offrire prodotti che promettono la sicurezza dei dati.

La "compatibilità privacy" sarà sempre più un valore essenziale anche per la qualità dei prodotti.

La privacy non è dunque solo un costo. È anche una importante risorsa.

Abbiamo, pertanto, salutato con soddisfazione la decisione del Governo precedente di non rinviare il termine per l'adozione dei documenti programmatici di

sicurezza. Questo necessario adempimento è stato avvertito da molti come "costoso" e "burocratico".

Non è così.

Esso risponde a una rilevante finalità: garantire al lavoratore, al cittadino, all'utente e al consumatore la tutela dei diritti fondamentali della personalità. Si pensi ai rischi per il lavoratore cagionati dall'uso di tecnologie produttive non regolate, o ai danni a cui può essere esposto l'utente o il consumatore dall'uso non protetto dei dati.

Ma vi è di più: l'adozione del documento programmatico stimola gli operatori ad assimilare la cultura della *privacy*.

È possibile semplificare alcune regole anche in questo campo. Siamo disposti a discuterne e per ciò abbiamo incontrato le associazioni di categoria e promosso una consultazione pubblica con gli operatori.

Abbiamo sempre detto, e qui lo ripetiamo, che vogliamo intensificare il dialogo con le imprese, le categorie economiche, i sindacati, le associazioni di rappresentanza, il mondo degli utenti e dei consumatori.

Vogliamo essere sostegno anche per coloro che svolgono attività professionali, collaborando con gli ordini e le categorie. Con questo intento, abbiamo avviato il tavolo per la redazione del codice deontologico sull'utilizzo dei dati nell'ambito dell'attività forense; abbiamo promosso un'attività di consultazione con i medici di base e con gli amministratori di condominio su provvedimenti che interessano tantissimi cittadini.

È con questo spirito che abbiamo monitorato l'attuazione del codice deontologico nel settore del credito al consumo; un settore che, nel 2005, ha movimentato una cifra pari a 76 miliardi di euro. Abbiamo regolato le attività di *marketing* e di profilazione nella grande distribuzione commerciale e nell'offerta di servizi di vario genere, vietando quelle svolte senza il consenso dei consumatori.

È in questo quadro che si collocano il provvedimento generale sulle cd. "carte di fedeltà", che sono oltre 30 milioni, e un recente provvedimento che ha vietato trattamenti illeciti nel settore alberghiero.

Abbiamo prestato la consueta attenzione alla tematica relativa alla tutela delle informazioni personali dei lavoratori, che presenta sempre nuove dimensioni e sfaccettature: ricordiamo, in particolare, l'utilizzo del sistema RFID che può determinare forme gravemente pervasive di controllo sulla vita del lavoratore.

Con riferimento alle relazioni tra cittadini e attività economiche, segnaliamo i provvedimenti sulle società di recupero crediti; sui rapporti dei cittadini con le compagnie assicurative; sulle corrette modalità di uso del *telepass*; sul rapporto tra utenti e servizi di radio-taxi. Massima cura abbiamo dedicato ad agevolare l'aggiornamento della normativa antiriciclaggio.

Tenendo presente la necessità di garantire la libertà di commercio e di circolazione dei beni, abbiamo rilasciato nuove autorizzazioni generali e dato esecuzione alle decisioni della Commissione europea sul trasferimento dati verso Paesi terzi, in applicazione dell'istituto delle clausole contrattuali tipo.

Intendiamo continuare ad impegnarci, insieme alle Autorità europee, sulla circolazione dei flussi transfrontalieri. Siamo convinti che la protezione dei dati non deve mai trasformarsi in una barriera che divida l'Europa dal resto del mondo.

Per questo, non ci siamo sottratti al confronto con i principali *privacy officer* di importanti multinazionali, alla ricerca di soluzioni che, senza pregiudicare il diritto alla protezione dei dati, consentano di fluidificare gli scambi fra Unione e Paesi terzi.

Un'esortazione alle grandi e medie imprese italiane: è poco diffusa la figura del *privacy officer*, ben conosciuta invece in altri Paesi. È il segno di una certa fatica ad adeguarsi ad una visione della protezione dati attiva e dinamica, essenziale per lo sviluppo del sistema Italia.

La *privacy* entra nell'Amministrazione Pubblica

Il 2005 è stato un anno particolarmente importante per la protezione dati nella Pubblica Amministrazione.

La trasformazione dell'Amministrazione, sotto la spinta dell'innovazione tec-

nologica, moltiplica reti e archivi informatici. È forte la tentazione efficientista ad interconnetterli fra loro, determinando una circolazione incontrollata dei dati e l'accesso indiscriminato da parte degli operatori.

L'Autorità si è misurata con questi fenomeni, affrontando la complessa vicenda nota come "Laziomatica". I provvedimenti prescrittivi e sanzionatori adottati sono un punto di riferimento non solo per i Comuni, ma per tutta l'Amministrazione: abbiamo dimostrato che è possibile far circolare i dati in rete senza duplicare gli archivi o accedere direttamente e indiscriminatamente alle banche dati.

Delicatissimo è, inoltre, il problema della protezione dei dati sensibili da parte della P.A., chiamata istituzionalmente a trattare una quantità enorme di dati riferiti alla salute, all'appartenenza etnica, alle opinioni e attività politiche e sindacali dei cittadini.

Uno dei successi più importanti dell'attività svolta nel 2005, e proseguita nel 2006, è l'aver favorito e ottenuto l'adempimento da parte delle Pubbliche Amministrazioni dell'obbligo di adottare i regolamenti per il trattamento dei dati sensibili.

Siamo grati al Governo precedente e a quello in carica per l'impegno dimostrato in risposta alle nostre sollecitazioni e consideriamo la proroga di recente approvata legata unicamente a ragioni obiettive derivanti dalle modifiche introdotte dal nuovo Governo nella struttura di alcuni Ministeri e Dipartimenti.

Comuni, Province, Regioni, Università, Camere di Commercio hanno risposto bene, così come moltissimi organi di rilevanza costituzionale, tutte le Autorità indipendenti, i grandi Enti nazionali e quasi tutti i Ministeri.

Il numero complessivo degli schemi di regolamento tipo relativi a categorie di enti e soggetti pubblici approvati supera la cinquantina. Ad essi si aggiungono centinaia di regolamenti adottati dai singoli enti sulla base degli schemi tipo.

Possiamo dire che nel 2005 la *privacy* ha fatto passi decisivi nella P.A.

È stata e continuerà ad essere un'occasione preziosa per le Amministrazioni

per ripensare se stesse, per riflettere sulle procedure interne, sulla funzionalità degli assetti organizzativi, sull'effettiva necessità dei dati di volta in volta richiesti.

É iniziata una nuova e più trasparente stagione nel rapporto fra Pubblica Amministrazione e cittadino.

Noi continueremo ad operare con scrupolo e con spirito collaborativo per verificare come il sistema amministrativo riuscirà a convertire le regole adottate in virtuosa prassi amministrativa.

Anche quest'anno, del resto, il rapporto di collaborazione del Garante con l'Amministrazione ha favorito l'adozione di soluzioni positive in settori strategici, come ad esempio in tema di monitoraggio della spesa sanitaria da parte del Ministero dell'Economia e delle finanze e di trattamento dei dati sensibili in materia sanitaria da parte delle Regioni.

Proprio la sanità ci ha impegnato molto e continuerà a impegnarci in futuro. I provvedimenti relativi all'organizzazione delle strutture sanitarie finalizzati a tutelare la riservatezza degli assistiti, quelli relativi all'attuazione della recente disciplina sulla procreazione assistita e all'informativa semplificata per i medici di base e pediatri ne sono esempio.

È prossima l'approvazione della autorizzazione generale in materia di trattamento dei dati genetici. All'orizzonte si affaccia il tema ancora in parte inesplorato della c.d. "sanità elettronica".

Impegnativa è stata l'attività nel settore specifico dell'amministrazione digitale. Abbiamo dato il parere sul nuovo codice dell'Amministrazione digitale, sul riutilizzo di documenti pubblici a fini privati, sul passaporto elettronico. Abbiamo avviato un'attività collaborativa con il CNIPA, che ha formato oggetto anche di un comune documento d'intenti. Essa ci ha consentito ad esempio di dare un importante parere preventivo sul bando di gara predisposto dal Ministero di Giustizia per la sicurezza di basi di dati strategiche nel contrasto alla criminalità organizzata.

L'innovazione tecnologica della P.A. è una linea di azione prioritaria per il Paese. Siamo pronti a fare la nostra parte.

La sicurezza nella società tecnologica

Un settore particolare è quello delle strutture e degli apparati di sicurezza e di prevenzione.

Le nostre società hanno bisogno di sicurezza.

L'Europa ha bisogno di sicurezza.

L'Unione Europea, nata per promuovere il libero mercato e svilupparsi come spazio di democrazia e libertà, ora dedica particolare attenzione alla tutela della sicurezza dei cittadini.

Sono sempre più forti le spinte ad avvalersi di tutte le opportunità informative offerte dalle tecnologie per ottenere un controllo generalizzato, preventivo e spesso pervasivo per finalità di sicurezza.

Le decisioni assunte dopo i fatti di Madrid e Londra hanno ampliato, sia nel nostro Paese che nell'Unione, la quantità e qualità dei dati conservati per ragioni di sicurezza.

L'Unione Europea ha adottato alla fine del 2005 una direttiva sulla c.d. "*data retention*", che comporterà la conservazione di miliardi e miliardi di informazioni, riguardanti aspetti essenziali della vita di relazione di tutti i cittadini europei. Si è calcolato che dovrebbero essere conservati ogni giorno 200 milioni di conversazioni, 300 milioni di "eventi" di telefonia mobile e 2 milioni e 400 mila gigabyte di dati annui solo per la posta elettronica.

Nel nostro Paese, dove già erano previsti tempi lunghissimi di conservazione dei dati di traffico telefonico, lo scorso anno con il c.d. decreto Pisanu si è esteso l'obbligo di conservazione anche ai dati di traffico telematico, sia pure per un tempo più breve.

Non è detto che più dati significhino maggior sicurezza.

Per questo Governo e Parlamento sono chiamati a verificare l'efficacia di tali misure, tanto più quando, come accade in Italia, i tempi di conservazione sono più lunghi di quelli previsti dall'Unione.

In ogni caso, questa massa di informazioni va adeguatamente salvaguardata, per garantire che sia usata soltanto dai soggetti autorizzati e per le finalità stabilite.

A ciò si aggiunge che l'*Europa della sicurezza* sta intensificando l'interconnessione fra le banche dati utilizzate per i controlli sui movimenti delle persone, per il contrasto all'immigrazione clandestina e al crimine. I nuovi sistemi SIS II e VIS II prevedono per la Commissione un ruolo penetrante di coordinamento dell'interoperabilità delle banche dati nazionali.

Alcuni Stati europei (Francia, Germania, Spagna, Belgio, Austria, Paesi Bassi e Lussemburgo) hanno recentemente sottoscritto a Prum, nell'ambito della cooperazione rafforzata, un Trattato che prevede anche la possibilità di scambiarsi informazioni riguardanti dati genetici. Si tratta di una problematica che anche in Italia dobbiamo affrontare con la massima attenzione alle ragioni e valutazioni di tutti.

Su questi temi abbiamo sempre adottato un atteggiamento altamente responsabile, attenti alle ragioni complessive e all'interesse generale.

La *privacy* non può essere un ostacolo alla sicurezza. Sicurezza e *privacy* sono parti coessenziali del sistema democratico.

Riteniamo così necessario che, come proposto dalla Commissione, l'adozione degli strumenti normativi relativi al rafforzamento della cooperazione giudiziaria e investigativa avvenga contestualmente all'approvazione di una robusta normativa sulla "*data protection*" anche nei settori della sicurezza e della giustizia.

Rivolgiamo un appello al Governo, ed in particolare al Ministro dell'interno e al Ministro della giustizia, affinché sostengano la posizione della Commissione, condivisa in modo unanime dal Gruppo europeo delle Autorità.

Ancora sul versante europeo. Dopo la recente decisione della Corte di Giustizia che, su ricorso del Parlamento europeo, ha annullato l'accordo fra UE e USA relativo al cd. PNR, è necessario negoziare un nuovo e più soddisfacente accordo sulla comunicazione dei dati dei cittadini europei in transito o in volo per gli Stati Uniti.

Su questi temi siamo stati sempre presenti sia nell'ambito del Gruppo dei Garanti europei sia nelle Conferenze internazionali delle Autorità di protezione dati: da Montreux a Madrid, da Budapest a Varsavia.

Sul versante delle strutture strumentali all'attività investigativa e di vigilanza, ci stiamo muovendo e intendiamo farlo ancora, sia con misure di tipo prescrittivo che con una adeguata attività di verifica della loro applicazione.

Da un lato, il nostro intervento, rispettoso delle competenze di ciascuno, può aiutare le strutture di sicurezza a rendere più efficaci le modalità di conservazione dei dati. Da un altro lato, la nostra azione può aiutare i cittadini ad avere maggiore fiducia nelle strutture di sicurezza.

È un compito importante anche perché tocca un settore delicatissimo, nel quale il diritto del cittadino di accedere ai dati che lo riguardano è affievolito.

In questa prospettiva, nel 2005 abbiamo avviato un'attività di ispezione sul Centro di elaborazione dati del Dipartimento di pubblica sicurezza del Ministero dell'interno. Si tratta di un'attività di controllo che in una prima fase è stata finalizzata a verificare le misure di protezione delle informazioni registrate e che ha già dato luogo ad un provvedimento contenente misure per il rafforzamento del sistema di sicurezza. Un secondo, più organico, provvedimento sul complesso di attività svolte dal Ced sarà adottato a breve, all'esito dell'attività.