Relazione2005

Discorso del Presidente
Francesco Pizzetti

Roma, 7 luglio 2006

www.garanteprivacy.it

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.

Privacy e pubblicazione delle intercettazioni telefoniche fra mezzi di informazione e autorità giudiziaria

Nel 2005, l'Autorità è intervenuta sulla libertà di informazione e sul tema della pubblicazione dei contenuti delle intercettazioni telefoniche. Fenomeno, questo, che ha conosciuto un continuo crescendo in queste ultime settimane.

Le decisioni del Garante sono sempre state improntate a cautela e prudenza, essendo in gioco tanto la libertà di informazione, sancita dall'art. 21 della Costituzione, quanto il diritto alla riservatezza e alla dignità, che trovano fondamento costituzionale nell'art. 2.

Valori costituzionali che vanno bilanciati e applicati in concreto alle singole fattispecie, tenendo conto di molteplici variabili.

Vengono in gioco la natura dell'informazione, l'oggetto e il soggetto, il contesto in cui viene resa la notizia e il diritto dei cittadini a conoscere tutto quanto è necessario sapere per esercitare un salutare controllo democratico.

È uno dei risvolti più nobili del mestiere di chi fa informazione, valutare se una notizia è essenziale per consentire all'opinione pubblica una conoscenza obiettiva dei fatti, o se invece è, oltre che irrilevante, anche lesiva della dignità personale.

Non è buon giornalismo, e comunque non è mai lecito, ledere la dignità delle persone per mero "*gossip*", utile ad aumentare le vendite o a solleticare forme di "*voyerismo*".

Nelle numerose decisioni adottate, abbiamo sempre cercato di contribuire a far sì che chi esercita un mestiere tanto delicato si ponga alcune domande, adotti filtri, si sforzi di valutare in modo scrupoloso l'impatto di un dettaglio o del riferimento ad una persona. In una parola, sia consapevole del ruolo fondamentale della libera informazione in una società democratica.

Non sono mancati interventi dell'Autorità di divieto e di blocco, anche con

riferimento a fatti riguardanti persone note o che svolgono funzioni pubbliche. Sempre abbiamo ribadito il rispetto del principio di essenzialità della notizia e della tutela della sfera privata, quali limiti invalicabili al corretto esercizio del diritto di cronaca.

Numerosi sono stati i provvedimenti a tutela di singoli cittadini adottati in seguito a ricorso. I più interessanti ci hanno permesso di precisare sia i principi relativi al diritto all'oblìo che quelli legati alla tutela dei minori.

Consentiteci, infine, un supplemento di riflessione sulla pubblicazione dei contenuti delle intercettazioni telefoniche.

Particolare clamore hanno suscitato di recente modalità e forme inedite di pubblicazione integrale dei contenuti delle intercettazioni, talvolta disponibili su Internet o raccolte in *dossier* posti in vendita.

Il fenomeno merita attenzione.

I testi delle intercettazioni finiscono in un brogliaccio contenente il riassunto delle conversazioni registrate, redatto da un operatore di giustizia, finalizzato ad essere conservato, valutato e utilizzato da altri operatori di giustizia (giudici e avvocati).

Pubblicare pressoché integralmente questo materiale in forma grezza, senza alcuna intermediazione e commento, non sempre è un servizio utile alla formazione di un libero e corretto convincimento del lettore.

Offrire all'opinione pubblica, senza adeguata mediazione, il contenuto di testi destinati alla diversa funzione di concorrere, insieme ad altri strumenti probatori, alla formazione del convincimento del pubblico ministero e/o del giudice, significa muoversi su un terreno minato.

Con il provvedimento generale, adottato alcuni giorni fa, abbiamo voluto ribadire con forza l'importanza delle regole che devono presiedere l'esercizio di un diritto-dovere di cronaca e d'informazione rispettoso della riservatezza e della dignità individuale, confermando orientamenti e indirizzi consolidati.

Nessuno, meno che mai il Garante, chiede censure preventive o bavagli all'informazione.

Chiediamo che il giornalista svolga fino in fondo il proprio mestiere, soppesando, anche rispetto a persone che hanno rilievo pubblico, le notizie e distinguendo fra informazioni necessarie per valutare il fatto e informazioni che invece attengono prevalentemente alla sfera privata del soggetto.

La posizione del "terzo incolpevole", dei familiari e dei minori deve essere sempre tutelata, così come particolare attenzione va prestata alle informazioni sensibili.

Siamo consapevoli che l'uso delle intercettazioni telefoniche investe anche la responsabilità di altri soggetti, in primo luogo gli operatori della giustizia.

Ed è per questo che abbiamo rivolto un nuovo caloroso invito al Consiglio Superiore della Magistratura affinché, nell'ambito delle sue competenze, si attivi perché siano migliorate le garanzie e le misure di sicurezza a tutela della riservatezza delle informazioni processuali.

Inoltre, ci siamo impegnati a collaborare su questi temi con Parlamento e Governo anche attivando il diritto-dovere di segnalazione che la legge ci attribuisce.

Quanto al nostro potere di controllo, che, per sua natura, è destinato sempre a svolgersi "a posteriori", riteniamo doveroso chiedere soprattutto al Parlamento una revisione normativa che preveda la possibilità per l'Autorità di comminare sanzioni amministrative di carattere pecuniario, qualora si accerti la violazione dei principi contenuti nel Codice deontologico.

Il Garante e i servizi di comunicazione elettronica

Nel 2005 la materia delle intercettazioni telefoniche è stata affrontata dal Garante anche sotto un altro profilo, parimenti importante.

In Italia, l'autorità giudiziaria fa un ampio ricorso a questo metodo investiga-

tivo, con la conseguenza che il numero delle intercettazioni, così come i relativi costi, sono, come ha ricordato di recente il Ministro di Giustizia, particolarmente alti, specialmente in confronto agli altri Paesi europei.

Va ricordato che, oltre alle intercettazioni telefoniche, l'autorità giudiziaria può chiedere ai fornitori del servizio molto altro, come la localizzazione delle chiamate e la realizzazione di intercettazioni ambientali. Inoltre vi sono le intercettazioni preventive svolte, su autorizzazione del magistrato, dalle forze di polizia.

Siamo di fronte a scelte del legislatore, prima, e dei singoli magistrati inquirenti, dopo. Non spetta a noi esprimere valutazioni al riguardo.

Sappiamo, però, che più si raccolgono dati personali, maggiore è il rischio che le misure di sicurezza non siano sufficienti ad assicurare la loro riservatezza.

È prioritario l'obbligo che i gestori telefonici adottino ferree misure di sicurezza e che l'autorità giudiziaria protegga le informazioni e i dati ottenuti.

Il Garante ha svolto un'attenta attività di accertamento sulle modalità con cui i gestori adempiono alle richieste dell'Autorità giudiziaria, fornendo il servizio indispensabile per l'attività di intercettazione.

Le verifiche hanno evidenziato la urgente necessità di incrementare in modo significativo i livelli di sicurezza dei sistemi e lo scorso dicembre il Garante ha prescritto numerose misure di sicurezza da adottare entro 180 giorni. Il termine fissato è ormai scaduto e ora verificheremo se le nostre prescrizioni sono state rispettate.

Allo stesso tempo, abbiamo sottolineato la necessità che misure analoghe siano adottate dagli uffici giudiziari e fin da marzo abbiamo deciso di promuovere un'attività collaborativa finalizzata a questo, chiedendo il sostegno del Consiglio Superiore della Magistratura e del Ministro della Giustizia.

I recentissimi episodi ci hanno spinto pochi giorni fa a rinnovare il nostro allarme.

L'attenzione e disponibilità manifestata dal Ministro della Giustizia e da auto-

revoli esponenti della magistratura requirente ci confortano.

Consideriamo, dunque, l'indagine conoscitiva decisa dalla Commissione Giustizia del Senato un'occasione preziosa, e, se ci sarà richiesto, assicuriamo il nostro contributo. Così come non mancheremo di darlo ad ogni altra iniziativa che Parlamento o Governo intendessero intraprendere.

Un altro profilo molto delicato riguarda le modalità di protezione dei dati di traffico telefonico, obbligatoriamente conservati dai gestori per 5 anni.

Abbiamo recentemente accertato, allo stato soltanto nei confronti del più importante gestore italiano, l'insufficienza di misure adeguate a protezione proprio di questi dati e dei relativi tabulati. In particolare, è risultato inadeguato il sistema di registrazione degli accessi ai *data-base,* e incompleto il sistema di tracciamento e di identificazione di coloro che possono accedervi. Abbiamo subito adottato un provvedimento dettagliato, indicando le necessarie misure e dato 120 giorni per attuarle.

Contestualmente abbiamo avviato un'attività istruttoria e programmato un'impegnativa attività ispettiva, finalizzate ad adottare un provvedimento generale sulla conservazione dei dati di traffico, così come previsto dall'art. 132 del nostro codice. Si tratta di un provvedimento che dovrà definire in modo organico le misure e gli accorgimenti che ciascun gestore dovrà introdurre per mettere in piena sicurezza le sue banche dati.

Ancora per quanto riguarda il settore dei gestori telefonici vanno ricordate altre due nostre attività in corso.

Negli scorsi mesi abbiamo emanato un provvedimento rivolto a tutti i gestori in ordine all'inquietante fenomeno dei servizi non richiesti quali, ad esempio, l'indebita attivazione di linee adsl. Si tratta di un provvedimento che riguarda da vicino anche i cd. *call center* e rispetto al quale verificheremo ora se le nostre prescrizioni sono state attuate.

Solo qualche settimana fa, abbiamo aperto un'istruttoria per verificare se,

come una recente ordinanza della Corte di Appello di Milano ha ritenuto in sede cautelare, vi siano state da parte di un gestore illecite attività di profilazione di ex abbonati passati ad altro gestore.

In questo settore, il 2005 è stato, dunque, un anno di grande impegno, intensificato in questi ultimi mesi. Esso aumenterà ancora nei prossimi.

Sulla tutela dei dati di comunicazione e sulla loro conservazione bisogna riflettere con attenzione, sforzandosi anche di ricercare soluzioni innovative, idonee ad assicurare maggiori garanzie.

Noi lo sentiamo come un dovere.

Un'ipotesi, che qualcuno invita a esplorare, potrebbe essere la creazione di una struttura pubblica, in cui i gestori, scaduto il periodo per la fatturazione, siano tenuti a far confluire i dati in loro possesso. Si tratta di una idea già avanzata in sede europea e che ha destato perplessità, ma sulla quale si potrebbe provare a ragionare. Tale struttura dovrebbe comunque essere sottoposta alla vigilanza della nostra Autorità e dovrebbe garantire il più rigoroso rispetto delle misure di sicurezza prescritte.

La tutela delle banche dati e il ruolo dell'Autorità

Una tematica più generale attiene alle garanzie da prevedere a tutela della sicurezza e integrità delle grandi banche dati che costituiscono, e sempre più costituiranno, porzione significativa dell'organizzazione sociale.

Sino ad oggi, le Autorità di protezione hanno svolto prevalentemente alcuni fondamentali compiti: garantire il diritto di accesso dei cittadini ai loro dati personali, assicurare la rigorosa applicazione della normativa a tutela dei diritti individuali lesi da trattamenti illeciti, favorire un'applicazione il più possibile "armonizzata" delle direttive europee e assicurare l'implementazione della normativa nazionale.

A questo si aggiunge, specialmente per il Garante italiano, un potere, più o meno legislativamente definito, di prescrizione generale sulle modalità con le quali la

normativa europea e nazionale va applicata nei diversi settori. La stessa attività di promozione dei codici di deontologia e di buona condotta si inscrive in questo contesto.

È ora giunto il momento di accentuare l'attenzione sulla problematica della messa in sicurezza delle informazioni contenute nelle grandi banche dati.

Occorre una svolta.

Tutte le Autorità europee ne avvertono l'esigenza.

Su questo terreno, in parte nuovo, il Garante italiano vuole essere in prima fila.

Se questa prospettiva è condivisa, è necessario individuare con chiarezza le banche dati da sottoporre a una più attenta vigilanza, isolando quelle di interesse nazionale operanti in settori di particolare rilevanza.

Le banche dati di traffico nell'ambito delle telecomunicazioni, così come quelle operanti nei settori della sicurezza e quelle contenenti campioni biometrici e del dna, dovrebbero certamente far parte del novero di queste strutture.

A tal proposito, dobbiamo fare presente che non hanno ancora trovato attuazione le previsioni del Codice che assegnano al Ministro della giustizia e al Ministro dell'interno il compito di individuare le banche dati centrali di cui si avvalgano le loro amministrazioni e la cui elencazione deve essere allegata al codice della *privacy*.

Tale individuazione, peraltro, potrebbe essere il primo passo per dar vita ad un apposito "registro delle banche dati ad alto rischio", che assolverebbe anche una funzione di trasparenza nei confronti dei cittadini.

Aggiungo che sarebbe anche importante che venisse data piena attuazione a quanto previsto dall'art. 58 del Codice privacy in materia di trattamento dati da parte degli organismi di difesa e sicurezza dello Stato.

Su un piano più generale, riteniamo peraltro utile invitare il Parlamento a riflettere sull'opportunità di individuare sedi e forme idonee per assicurare un dialogo costante fra il luogo della democrazia rappresentativa e un'Autorità come la nostra che, per la sua natura e per vincolo comunitario, non può che essere ed agire come Autorità indipendente, ma che ha e deve avere nel Parlamento il suo interlocutore privilegiato.

Ed è per questo che riteniamo sia giusto esprimere qui la nostra consapevolezza che, di fronte alla complessità e all'ampiezza degli obiettivi che ci proponiamo, i poteri dell'Autorità sono insufficienti.

Occorrono necessarie modifiche normative in relazione agli strumenti ispettivi e alle misure prescrittive e sanzionatorie. In particolare, è necessario attribuire all'Autorità il potere di irrogare sanzioni pecuniarie di carattere amministrativo in misura maggiore e in un numero di casi più ampio di quelli oggi tipizzati dal Codice. Occorre, inoltre, un ripensamento delle strutture organizzative e della dotazione organica dell'Autorità. Attualmente, essa si avvale di un Ufficio di supporto composto da circa cento unità. Troppo poco per poter operare come Autorità pienamente capace di garantire anche il corretto funzionamento delle grandi banche dati.

Altri settori di intervento dell'Autorità nel corso del 2005

È ora di avviarci alla conclusione.

Come negli anni precedenti, anche nel 2005 siamo intervenuti in molteplici ambiti, sia in seguito a istanze dei singoli cittadini, associazioni, ordini professionali e categorie, sia *ex officio*.

I dati dimostrano che il Garante rappresenta un'Autorità peculiare nel panorama delle c.d. Autorità indipendenti.

L'elemento distintivo di maggiore evidenza attiene al rapporto 'simbiotico' fra l'Autorità e la materia "*privacy*", che ha al suo centro il diritto fondamentale del cittadino alla protezione dei suoi dati personali.

Il Garante non è chiamato a regolare un settore specifico.

A noi spetta promuovere e accompagnare l'assimilazione e il radicamento di un nuovo modo di trattare le informazioni personali da parte di una platea vastissima di soggetti. Il nostro compito ultimo è di concorrere a garantire non solo il

rispetto della libertà e dignità dei singoli, ma anche il rafforzamento del quadro democratico del Paese.

La complessità e la ricchezza del nostro operato deriva dall'ampiezza e trasversalità dei settori su cui siamo chiamati a intervenire.

Di qui l'elevata quantità di pronunce, pareri, provvedimenti emessi in quest'anno e la nutrita serie di decisioni legate alla nostra attività di controllo, di regolazione, di stimolo verso i decisori pubblici e privati.

Alcuni numeri. Nel solo 2005 l'Autorità ha adottato 724 provvedimenti collegiali, che hanno riguardato anche la trattazione di 634 ricorsi. Considerando anche alcuni casi trattati nell'anno e definiti più di recente, ha risposto a 1633 reclami e segnalazioni e a 364 quesiti; ha dato 31 pareri su atti normativi del Governo; ha approvato 61 schemi di regolamento sul trattamento dei dati sensibili nella P.A.. I provvedimenti generali sono stati più di un centinaio, fra cui il rinnovo di sette autorizzazioni generali.

Abbiamo dedicato tempo ed energie all'ascolto delle categorie economiche e produttive, degli ordini professionali, dei consumatori.

Auspichiamo che la *privacy* sia sentita come un aspetto positivo della vita e per questo abbiamo avviato una riflessione sul rapporto fra *privacy* e felicità.

Abbiamo svolto un'intensa attività per dotare l'Autorità dei regolamenti indispensabili per il suo funzionamento, in modo da irrobustirne la struttura e l'organizzazione e da aumentare le garanzie dei cittadini che si rivolgono a noi.

Abbiamo innovato nel metodo di lavoro, introducendo la programmazione semestrale degli affari da trattare e delle attività ispettive.

Duecento ispezioni nel corso del 2005 e centoquarantacinque solo nel primo semestre di quest'anno testimoniano l'importanza che ha per noi quest'attività. Intendiamo continuare su questa via, rafforzando sempre di più la collaborazione con la Guardia di Finanza. Collaborazione fattiva e preziosa, della quale voglio qui ringraziare il Comandante del Corpo, gli alti ufficiali e tutti coloro che lavorano con noi.

Conclusione

Signor Presidente,

Signore e Signori.

Insieme ai miei colleghi, Giuseppe Chiaravalloti, Mauro Paissan e Giuseppe Fortunato, mi auguro di aver dato un riassunto fedele della nostra attività, delle nostre riflessioni, delle prospettive che ci poniamo.

Vogliamo assicurare Lei, Signor Presidente, il Parlamento e il Governo che non verremo mai meno ai doveri e compiti assegnati.

Il Garante si muove sul crinale più sensibile della società a "cambiamento velocissimo": la linea di confine fra democrazia e libertà da un lato, controllo e paura dall'altro.

Il Garante opera perché si continui a vivere in una comunità di donne e di uomini liberi, responsabili, capaci di usare la tecnica senza diventarne prigionieri, impegnati a costruire la propria sicurezza senza rinunciare alla loro dignità di uomini.

Chiediamo al Paese e al Parlamento fiducia e lavoriamo per dare fiducia.