Senato della Repubblica XV LEGISLATURA

Giunte e Commissioni

RESOCONTO STENOGRAFICO n. 1

N.B. I resoconti stenografici delle sedute di ciascuna indagine conoscitiva seguono una numerazione indipendente.

1ª COMMISSIONE PERMANENTE (Affari costituzionali, affari della Presidenza del Consiglio e dell'interno, ordinamento generale dello Stato e della Pubblica amministrazione)

INDAGINE CONOSCITIVA SUI RAPPORTI TRA LIBERTÀ DI INFORMAZIONE, SVILUPPO DELLE COMUNICAZIONI, TUTELA DEI DIRITTI DELLA PERSONA E SICUREZZA PUBBLICA

58ª seduta (pomeridiana): mercoledì 29 novembre 2006

Presidenza del presidente BIANCO

IC 0192
TIPOGRAFIA DEL SENATO (310)

I N D I C E

Audizione del Presidente dell'Autorità garante per la protezione dei dati personali

N.B. L'asterisco accanto al nome riportato nell'indice della seduta indica che gli interventi sono stati rivisti dagli oratori.

Sigle dei Gruppi parlamentari: Alleanza Nazionale: AN; Democrazia Cristiana-Partito repubblicano italiano-Indipendenti-Movimento per l'Autonomia: DC-PRI-IND-MPA; Forza Italia: FI; Insieme con l'Unione Verdi-Comunisti Italiani: IU-Verdi-Com; Lega Nord Padania: LNP; L'Ulivo: Ulivo; Per le Autonomie: Aut; Rifondazione Comunista-Sinistra Europea: RC-SE; Unione dei Democraticicristiani e di Centro (UDC): UDC; Misto: Misto; Misto-Italia dei Valori: Misto-IdV; Misto-Italiani nel mondo: Misto-Inm; Misto-L'Italia di mezzo: Misto-Idm; Misto-Partito Democratico Meridionale (PDM): Misto-PDM; Misto-Popolari-Udeur: Misto-Pop-Udeur.

Interviene il professore Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali, accompagnato da Mario de Bernart, Baldo Meo, Luigi Montuori, Veronica Nicotra e Laura Tempestini.

I lavori hanno inizio alle ore 17.

PROCEDURE INFORMATIVE

Audizione del Presidente dell'Autorità garante per la protezione dei dati personali

PRESIDENTE. L'ordine del giorno reca l'indagine conoscitiva sui rapporti tra libertà di informazione, sviluppo delle comunicazioni, tutela dei diritti della persona e sicurezza pubblica.

Comunico che, ai sensi dell'articolo 33, comma 4, del Regolamento, è stata chiesta l'attivazione dell'impianto audiovisivo e che la Presidenza del Senato ha già preventivamente fatto conoscere il proprio assenso. Se non ci sono osservazioni, tale forma di pubblicità è dunque adottata per il prosieguo dei lavori.

È oggi in programma l'audizione del professor Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali, che ringrazio per la disponibilità dimostrata accogliendo il nostro invito.

L'audizione di oggi è stata fortemente voluta dai membri di questa Commissione, nonostante la necessità di superare alcuni problemi procedurali. Tutti i Gruppi, sia di maggioranza che di opposizione, hanno reputato importante avere la possibilità di ascoltare il Presidente dell'Autorità garante per la protezione dei dati personali dei cittadini, per le parti di competenza di questa Commissione. Nel corso dell'audizione non ci occuperemo infatti degli argomenti di stretta competenza della Commissione giustizia in quanto non siamo interessati agli aspetti di procedura penale se non per i riflessi che gli stessi possono avere sulle tematiche di nostra competenza. Mi riferisco alla delicata questione attinente la sicurezza del Paese e la tutela dei diritti costituzionalmente garantiti, a partire dal diritto alla riservatezza. Pertanto l'attività delicatissima affidata all'Autorità da lei presieduta è per questa Commissione di grande rilievo; quindi, nei termini e nei modi previsti dal Regolamento del Senato, credo che avremo modo di ascoltarla ancora.

Invito il presidente Pizzetti a svolgere una relazione introduttiva per illustrare l'organizzazione, le funzioni e le modalità di svolgimento della sua delicata attività, ivi inclusi i problemi che sta attualmente affrontando. Potremmo intervenire sulla materia anche *de iure condendo*, con iniziative legislative appropriate, per consentire all'Autorità di svolgere al meglio le

delicate funzioni che le sono affidate. La pregherei pertanto di tener conto anche della possibilità che il Parlamento preveda interventi idonei a migliorare dal punto di vista organizzativo, funzionale e legislativo l'operatività dell'Autorità che lei presiede.

Do quindi la parola al professor Pizzetti che svolgerà una relazione introduttiva.

PIZZETTI. Ringrazio il Presidente e la Commissione per l'invito che ci è stato rivolto e che ci offre l'occasione di essere presenti in una sede importante ed autorevole come il Senato per spiegare chi siamo, cosa facciamo e i problemi che dobbiamo affrontare.

Considero l'iniziativa di questa Commissione di avviare l'indagine conoscitiva in titolo molto importante, essendo fondamentale per le autorità in genere, e in particolare per la nostra, mantenere un costante rapporto con il Parlamento, al fine di rappresentare i problemi che abbiamo di fronte e di ascoltare i suggerimenti del legislatore e dei rappresentanti del popolo italiano in ordine alle problematiche che siamo chiamati ad affrontare. D'altra parte, la nostra Autorità è interamente di nomina parlamentare. Per quanto mi riguarda, essendo stato eletto dal Senato, considero importantissimo il rapporto con le due Assemblee legislative, e soprattutto con questa, che rappresenta la culla della mia nomina. Ritengo, pertanto, che questa Commissione rappresenti la sede più adatta per un continuo e costante rapporto con il Parlamento, che non può certo esaurirsi nella relazione annuale, per quanto prevista dalla legge e ritenuta un'occasione rituale di grande importanza.

Innanzi tutto vorrei illustrare gli aspetti essenziali della nostra attività. Come sapete, siamo noti come Autorità per la *privacy*, ma in realtà siamo l'Autorità garante per la protezione dei dati personali dei cittadini, definizione meno immediatamente comprensibile per la sua freddezza, ma che assume sempre maggiore rilevanza concernendo la tutela di tutti i dati e le informazioni che ci riguardano. La conoscenza di questi dati, infatti, permette di conoscere i rilievi dei nostri comportamenti e del nostro modo di essere. Trattandosi di attività che presenta aspetti, specificità e particolarità terribilmente pervasivi, siamo chiamati a difendere la libertà dei cittadini di potersi muovere, vivere e operare senza che le informazioni che li riguardano siano continuamente conosciute, trattate e analizzate da chi non ha il diritto di conoscerle ed utilizzarle. Soprattutto siamo chiamati a fare in modo che tali informazioni non vengano utilizzate contro il cittadino per limitarne la libertà, trasformando una società di uomini liberi in una società di controllati.

La nostra Autorità ha lo specifico compito istituzionale di tutelare un diritto fondamentale dei cittadini. La particolarità della cultura europea è di considerare diritto fondamentale dei cittadini europei la protezione dei dati che li riguardano. Ciò è stabilito dalla Convenzione n. 108 del Consiglio d'Europa, dalla Carta dei diritti dell'Unione europea e dal Trattato costituente per l'Europa che il Parlamento italiano ha ratificato. La specificità è che la protezione dei dati personali nell'Unione europea rappresenta

un diritto fondamentale riconosciuto. A presidio di questo diritto fondamentale sono istituite le Autorità nazionali che formano insieme nel *working party* (articolo 29), il Collegio delle Autorità garanti dell'Unione europea.

Gli elementi principali che presidiano la tutela di questo diritto fondamentale del cittadino sono – come noto – i seguenti: il diritto del cittadino a dare un consenso informato affinché i propri dati possano essere utilizzati; il diritto ad avere la garanzia che i propri dati siano utilizzati per finalità definite, rispetto alle quali si chiede il suo consenso, in base al principio di adeguatezza, di proporzionalità e di necessità; il diritto ad avere garanzia che i dati di cui altri soggetti vengono a conoscenza sulla base di questi princìpi siano protetti. La protezione dei dati è elemento essenziale. Ne consegue che la garanzia dei diritti suindicati è possibile nella misura in cui chi ne ha la disponibilità ne garantisce anche la protezione da accessi illegittimi e da autorizzazioni non conformi a quanto portato a conoscenza del soggetto interessato o sulle quali quest'ultimo non ha espresso il proprio consenso.

Ovviamente la garanzia vale anche in caso di trasferimento dei dati personali all'estero, soprattutto se si tratta di Paesi in cui non è prevista una protezione adeguata e conforme alla normativa europea.

In questo quadro, uno degli aspetti fondamentali della nostra attività è il diritto dei cittadini a sapere quali sono i dati posseduti dal soggetto che ne ha la disponibilità, per quale finalità sono utilizzati e attraverso quale modalità di trattamento. Il diritto di accesso alla conoscenza dei dati personali è garantito dalla nostra Autorità con un procedimento specifico, estremamente veloce, che si attiva sulla base di un ricorso del cittadino. In altri termini, può rivolgersi a noi il cittadino che non ha ottenuto una risposta soddisfacente alla sua richiesta di conoscere i dati che lo riguardano in possesso di altri soggetti. Con un procedimento molto rapido, che dura al massimo 60 giorni, garantiamo che questo diritto di accesso si trasformi nel rispetto concreto della domanda di conoscibilità dei dati.

I cittadini hanno anche la possibilità di segnalare all'Autorità che il trattamento dei loro dati è, a loro giudizio, illecito o non conforme alla legge. Chiude il sistema il potere generale dell'Autorità di verificare le modalità con cui vengono trattati i dati dei cittadini e le garanzie con cui gli stessi sono protetti.

Il cuore del ruolo dell'Autorità sta tradizionalmente nel rapporto tra Autorità e cittadini. È importante sottolineare che sono previste alcune deroghe rispetto a determinati settori o funzioni, prevalentemente pubblici. Non è richiesto, ad esempio, il consenso del cittadino quando il dato è trattato dalla pubblica amministrazione per finalità di interesse pubblico e per ragioni di giustizia, di pubblica sicurezza, di difesa e sicurezza dello Stato. Non solo, il diritto di accesso del cittadino è affievolito nel caso di dati trattati per ragioni di giustizia, di polizia e sicurezza, di difesa e sicurezza dello Stato. Mi riferisco quindi a tutti gli apparati giudiziari, di polizia e dei servizi di sicurezza, i quali ultimi sono richiamati nel concetto di difesa e sicurezza dello Stato. In questi casi non c'è il diritto di

accesso diretto del cittadino, così come non c'è quello al consenso informato. In relazione ai trattamenti giudiziari e ai normali ricorsi previsti dai codici di rito, rispetto alle Forze di polizia e, in particolare, ai servizi di sicurezza, il cittadino deve rivolgersi al Garante, affinché verifichi se queste strutture hanno dati che lo riguardano ed eventualmente se gli stessi sono trattati conformemente alla legge. Rispetto a tali settori il ruolo dell'Autorità è ancora più incisivo: garantire i cittadini che non possono garantirsi da soli.

L'Autorità non si limita a rendere concreto un diritto di accesso che il cittadino ha in base alla legge, ma garantisce anche che i dati in possesso degli apparati di sicurezza e di difesa dello Stato siano trattati conformemente alle leggi. Rispetto ai settori giustizia, Forze di polizia, difesa e sicurezza dello Stato si accentua il nostro ruolo di verifica e di controllo sulle modalità di protezione e tutela dei dati, proprio perché questi ultimi sono utilizzati per funzioni pubbliche, che prevalgono sull'interesse del cittadino a conoscere come e quali dati sono conservati ed utilizzati. A maggior ragione, i dati utilizzati a tale scopo devono essere protetti con misure di sicurezza adeguate.

A ciò si aggiunge una specifica competenza in materia di telecomunicazioni, soprattutto con riferimento ai dati di traffico telefonico e telematico. Una specifica norma del codice sulla *privacy* affida all'Autorità il compito di adottare un provvedimento generale che detti ai gestori telefonici le specifiche da adottare al fine di garantire ai cittadini che i dati di traffico – che sono di una delicatezza estrema, più di quanto lo siano le intercettazioni telefoniche – possano essere conservati dai gestori telefonici e acquisiti dall'Autorità giudiziaria per il periodo successivo stabilito dal legislatore.

Merita inoltre richiamare l'attenzione di questa Commissione su una normativa che caratterizza la nostra Autorità e che non si riscontra con analoga incisività negli altri ordinamenti europei. Detta normativa attribuisce all'Autorità specifiche competenze in materia di libertà di stampa e di cronaca, a cui è connesso l'esercizio di un diritto costituzionalmente garantito che si sostanzia nel diritto dei cittadini ad essere informati e nel diritto dei mezzi di informazione ad informare. Va ricordato, però, che a livello costituzionale emerge prima di tutto il diritto ad essere informati e che rispetto ad esso il diritto di informare è strumentale. Si tratta infatti di un diritto costituzionale fondamentale in una democrazia, in assenza del quale quest'ultima non solo è incompiuta, ma inesistente. Questo diritto fondamentale deve trovare armonizzazione con il diritto, altrettanto fondamentale, dei cittadini alla riservatezza e alla dignità della loro persona. Si pone, pertanto, un delicatissimo problema di armonizzazione tra due diritti, entrambi costituzionali e fondamentali.

La specificità italiana è che l'Autorità ha una competenza particolarmente incisiva proprio nell'individuazione del punto di equilibrio tra questi due diritti. Il nostro codice richiama princìpi – peraltro stabiliti in sede giurisdizionale – circa l'essenzialità dell'informazione, la finalizzazione del diritto di cronaca a far conoscere fatti di interesse pubblico, l'attiva-

zione sulla base di comunicazioni dell'interessato o attraverso comportamenti pubblici tenuti dall'interessato. Si stabilisce altresì un codice deontologico che deve essere adottato – così come di fatto è stato – di comune intesa tra l'ordine dei giornalisti e l'Autorità garante, alla quale sono rimesse le misure ulteriori da adottare per garantire che il diritto di cronaca sia esercitato nel rispetto dei dati sensibili e, in particolare, di quello relativo alla vita sessuale dei cittadini, dati che richiedono una maggiore e più mirata garanzia e tutela.

Come comprenderete, il ruolo dell'Autorità è davvero rilevante perché attiene: alla tutela del diritto fondamentale del singolo cittadino alla protezione dei suoi dati, secondo i princìpi di riservatezza, dignità e rispetto dei diritti fondamentali; alla verifica che tali dati siano trattati e protetti secondo la normativa, siano garantiti da accessi illeciti ed illegittimi e siano usati nell'interesse dei cittadini e non contro di loro. All'Autorità viene attribuito un ruolo specifico nei settori della sicurezza, della giustizia e dei servizi di sicurezza dello Stato, di cui abbiamo parlato, oltre che un ruolo delicatissimo in ordine all'informazione e all'equilibrio tra libertà di informazione e diritto alla riservatezza.

L'Autorità sta per compiere dieci anni: nel 2007 ricorrerà il decennale della sua istituzione. Questi dieci anni hanno cambiato il mondo e con esso lo scenario in cui l'Autorità opera. Conseguentemente, dall'avere principalmente un ruolo di tutela individuale del cittadino, titolare del diritto fondamentale alla protezione dei dati che lo riguardano, l'Autorità ha visto ampliarsi progressivamente il suo dovere di garantire che la nostra società rimanga democratica, libera e sicura senza trasformarsi in una società di controllati e senza perdere la propria libertà. La protezione dei dati, oltre ad essere un diritto fondamentale dei singoli cittadini, sta diventando un elemento essenziale che caratterizza il tipo di società. Ci muoviamo sempre più sul crinale, delicatissimo, che separa una società libera, che garantisce la sicurezza dei cittadini, da una società che, pur di essere sicura, accetta di perdere la libertà e di trasformarsi in una società di controllati. Questo fenomeno si sta verificando in misura sempre più significativa per una pluralità di circostanze, la prima delle quali e la più rilevante è che dal famoso 11 settembre del 2001 – in realtà, in seguito alle nuove tensioni che si sono delineate nel mondo e alla evoluzione delle vecchie –, la sicurezza non è più solo una funzione, ma spesso è anche una finalità. Il codice era stato immaginato in una società in cui alcuni apparati svolgevano compiti di polizia, giustizia e sicurezza, quali funzioni pubbliche. Oggi, sempre più spesso, ci troviamo di fronte a situazioni nelle quali il trattamento dei dati dei cittadini è finalizzato a garantire la sicurezza. Da funzione di un apparato la sicurezza diventa anche finalità del trattamento.

Le famose videocamere nelle metropolitane non rappresentano più un trattamento dei dati del cittadino per finalità di volta in volta individuate rispetto alle quali il cittadino può anche esprimere il suo consenso, e ciò in quanto quei dati vengono trattati al fine di garantire la sicurezza. Si tende ad estendere la normativa che «diminuiva» la tutela del diritto

alla *privacy* rispetto ad alcune funzioni pubbliche (come studiavamo nel diritto amministrativo dei nostri tempi) alla finalità di sicurezza. In altri termini, se si vuole essere sicuri di non perdere la vita in metropolitana a causa dell'esplosione di una bomba, bisogna rinunciare ad una parte di libertà, accettando la presenza di videocamere che controllano, in quanto in casi del genere la finalità del controllo equivale alla sicurezza.

Di fronte a questi cambiamenti il nostro compito è sempre più difficile. Con crescente frequenza siamo chiamati a una prudente analisi del rapporto fra la libertà e il diritto individuale alla tutela e alla protezione dei dati personali, distinguendo i casi in cui il trattamento dei dati necessita del consenso del soggetto interessato e quelli in cui, stante la crescente finalità di carattere generale della sicurezza, il consenso non è richiesto. È sempre più difficile trovare un punto di equilibrio convincente e accettabile. Per questo motivo abbiamo bisogno di un ampio dibattito pubblico e di una presa di coscienza collettiva.

Rispetto a questo quadro, è importante accentuare il nostro ruolo di protezione dei dati. I dati, infatti, sempre più spesso possono essere utilizzati per finalità di interesse generale, ricomprese in un generico bisogno di sicurezza. Conseguentemente, l'Autorità di garanzia, non potendo più essere sicura di poter difendere i cittadini vietando l'acquisizione dei dati, deve riuscire ad accentuare la sua capacità di controllo sull'uso che ne viene fatto, su come sono protetti, su chi ne viene a conoscenza, sulle banche dati in cui vengono inseriti e sulle modalità con cui sono trattati. Di fronte alla crescente necessità di accettare che il dato possa essere raccolto, bisogna proteggerlo garantendo che sarà usato solo per le finalità di volta in volta individuate dal legislatore. A tal fine bisogna censire e verificare le banche dati e capire come sono organizzate e protette da accessi illegittimi. Di qui la motivazione del mutamento che è in atto e di cui si percepisce l'evoluzione anche all'esterno.

Per questa ragione la nostra Autorità vuole accentuare sempre più il suo ruolo di controllo e di verifica. Non a caso anche nella finanziaria, al vostro esame in questi giorni, è contenuta una norma, che mi permetto di richiamare alla vostra attenzione e sulla quale chiedo il vostro consenso. Tale norma prevede l'aumento dell'organico dell'Autorità, specificamente collegato alla necessità di accentuare l'attività di verifica e di controllo: la nuova frontiera verso cui ci muoviamo non può che essere particolarmente attenta al controllo delle banche dati, in particolare di quelle di rilievo nazionale.

Questo scenario, che è di carattere generale, è accentuato non solo dai problemi connessi alla sicurezza della comunità, ma anche dalle innovazioni tecnologiche, che consentono in misura crescente la raccolta di dati e la trasformazione di dati biometrici in dati utilizzabili e trasferibili con tecnologie informatiche. L'impronta digitale è trasformabile in una sequenza informatica trasferibile attraverso una *e-mail*; così il profilo genetico, il codice alfanumerico che individua il DNA. Aspetti delicatissimi, che attengono alla sfera più intima della nostra corporeità, si trasformano con le nuove tecnologie sempre più in dati conoscibili, trattabili, archivia-

bili, trasmissibili, incrociabili, profilabili. Si pone nuovamente il problema del controllo, della verifica, della protezione, di come questi dati sono raccolti, chi li conserva e per quanto tempo, come si garantisce che non siano rubati o utilizzati contro il cittadino.

Entrando nel merito di alcuni fatti recenti, faccio presente che il nuovo collegio, in carica dall'aprile del 2005, aveva già ben presente questo quadro generale e fin dal mese di giugno del 2005 ha introdotto una innovazione ben comprensibile, alla luce della situazione che ho cercato di ricostruire. Mi riferisco a una accentuazione dell'attività ispettiva, con la previsione di una programmazione semestrale dell'attività di verifica e controllo su come e da chi i dati sono conservati, protetti e trattati. Già ci stavamo muovendo in questa direzione quando, come Autorità, siamo stati coinvolti (oserei dire quasi travolti, per fortuna non proprio, visto che siamo riusciti a reggere l'impatto) dalle emergenze che nel nostro Paese hanno caratterizzato il periodo che va dall'estate 2005 ad oggi.

Ricorderete benissimo la valanga di intercettazioni telefoniche pubblicate sui mezzi di diffusione a stampa, che hanno richiamato improvvisamente l'attenzione dell'opinione pubblica sul fenomeno. Le vicende che ho richiamato erano legate a intercettazioni telefoniche prevalentemente legittime, richieste dall'autorità giudiziaria secondo il codice di rito, che i gestori telefonici avevano effettuato secondo quanto prevede il nostro codice di procedura penale.

Tali vicende hanno sollevato interrogativi sotto due profili. Il primo concerne il loro legittimo utilizzo nell'ambito dell'esercizio del diritto di cronaca. Ci siamo trovati esposti, in prima fila rispetto a un fenomeno molto frequente, a dover ricercare il punto di equilibrio tra tutela della riservatezza e diritto di cronaca. Tema delicatissimo, dal momento che la nostra Costituzione vieta che la stampa sia sottoposta a censura o ad autorizzazione. In un quadro costituzionale che privilegia la libertà di informazione, decidere di vietare la pubblicazione di una informazione (che non significa «censurare» in senso tecnico, ma certo vi assomiglia molto) vuol dire avere un potere di una delicatezza estrema. Tale potere si spiega in relazione al diritto alla protezione della riservatezza del cittadino, che successivamente alla stesura della Carta costituzionale è stato tipizzato come un diritto fondamentale, oltre ad essere riconducibile agli articoli 2 e 3 della Costituzione stessa.

Questo fenomeno di massa ha investito l'Autorità con elevata frequenza. Ad esso si è fatto fronte attivando la prudenza e la saggezza che hanno sempre caratterizzato il collegio dell'Autorità, soprattutto nelle esperienze precedenti; e noi speriamo di esserne stati degni eredi. Di volta in volta, di fronte a un fenomeno in crescita (intercettazioni nel mondo del calcio, dei processi instaurati a Potenza, e via discorrendo), abbiamo sempre cercato di individuare il corretto punto di equilibrio.

Ovviamente, il fenomeno della pubblicazione delle intercettazioni telefoniche, prevalentemente disposte dalla autorità giudiziaria per fini di giustizia, ci ha posto i seguenti interrogativi: com'è possibile che il contenuto delle intercettazioni sia sempre conosciuto? Sono sempre legittime?

Il sistema di conservazione e di raccolta delle intercettazioni disposto dagli Uffici giudiziari, è sufficientemente protetto da accessi illeciti? Oltre ad essere possibili intercettazioni illegittime, si possono verificare accessi illeciti a intercettazioni legittime?

Nell'ambito della nostra competenza questa problematica si è trasformata nel dovere, da noi avvertito, di procedere ad un'attenta analisi e attività conoscitiva per poi impartire delle prescrizioni nei confronti dei gestori telefonici.

L'intercettazione telefonica avviene con un meccanismo paragonabile a un ponte: un giudice chiede che un determinato soggetto sia sottoposto ad intercettazione; un gestore lo consente attivando i mezzi tecnici necessari. Si crea una sorta di ponte i cui due pilastri sono il gestore e il giudice. Ovviamente, se i due pilastri non sono in sicurezza e vi sono fughe di notizie, da una parte o dall'altra, possono verificarsi intercettazioni legittime conosciute in modo illecito e rese note attraverso un'attività non lecita oppure intercettazioni illegittime, nel qual caso si esce dal rapporto gestore-giudice, posto che in presenza di intercettazione illecita il giudice non ha alcun ruolo.

Dall'agosto 2005, con un'attività durata mesi e tuttora in corso, abbiamo dapprima raccolto le informazioni necessarie e quindi adottato i provvedimenti relativi, vigilando sull'attuazione degli stessi. Ancora oggi abbiamo fissato un'ultima proroga, con scadenza 31 dicembre, finalizzata a far sì che i gestori telefonici adottino tutte le misure di sicurezza necessarie a garantire che le intercettazioni legittime, la conoscenza dei dati di traffico, le intercettazioni ambientali, la conoscenza di SMS e altri dati e-*mail* richiesti dai giudici siano forniti agli stessi in modo da evitare, nei limiti del possibile, la fuga di notizie sul versante dei gestori.

Il problema però troverà soluzione solo se anche l'autorità giudiziaria adotterà le necessarie misure di sicurezza. Al riguardo lo scorso marzo abbiamo prima scritto una lettera al CSM e una al ministro Castelli poi reiterato la richiesta al nuovo Governo e al CSM. In particolare abbiamo suggerito l'attivazione di un tavolo tecnico con il Ministero della giustizia e il CSM, assicurando la nostra piena disponibilità a collaborare. Ebbene, oggi invochiamo l'attenzione del legislatore e del Governo, affinché anche l'autorità giudiziaria adotti le misure di sicurezza necessarie nell'interesse della giustizia prima ancora che del cittadino stesso. È evidente, infatti, che se vi è una fuga di notizie, il primo a subire una conseguenza negativa è proprio il giudice inquirente, che si trova ad avere in mano l'arma dell'intercettazione spuntata, dal momento che l'intercettato sa di essere sottoposto a questa attività investigativa.

Non posso che ribadire l'augurio che l'autorità giudiziaria, di cui abbiamo chiare le difficoltà per la sua natura di potere diffuso su tutto il territorio, compia ogni sforzo per corrispondere a questa necessità, proprio nell'interesse della giustizia.

Abbiamo assistito, ed assistiamo continuamente, a un'imponente attività di formazione di dossier e di spionaggio sui dati contenuti nelle banche dati pubbliche. L'attività che più ha richiamato la nostra attenzione è

il trattamento illecito dei dati relativi al traffico telefonico. Ho parlato poc'anzi dell'enorme delicatezza dei dati di traffico telefonico contenenti una quantità impressionante di informazioni sugli utenti. Questo problema è emerso con forza in seguito al susseguirsi di vicende inquietanti che hanno portato nelle aule giudiziarie, e quindi all'attenzione di alcuni procuratori, fenomeni di accesso illecito, che hanno dato vita alla costituzione di quelle che ormai, con un brutto termine, chiamiamo attività di dossieraggio. Anche su questo versante siamo impegnati da tempo e siamo intervenuti con un'attività ispettiva il 20 dicembre 2005. A seguito poi di un ricorso relativo al caso specifico di un cittadino che aveva ricevuto a casa in forma anonima dati di traffico telefonico che lo riguardavano, abbiamo svolto una attività ispettiva presso la sede del gestore interessato. Alla suddetta attività ispettiva ha fatto seguito un provvedimento che ha imposto al gestore di adottare una serie di misure, necessarie a proteggere l'utente dal ripetersi di fenomeni di accesso illecito a dati di traffico dei cittadini. Il provvedimento ha stabilito un termine di 120 giorni, già scaduto, per l'adozione di dette misure. È attualmente alla nostra attenzione la relazione elaborata al riguardo. Abbiamo svolto due visite ispettive per constatare se quanto dichiarato corrisponde al vero. C'è stata chiesta anche un'ulteriore proroga che probabilmente concederemo. Abbiamo constatato che è stato fatto un investimento massiccio (circa 30 milioni di euro, su dichiarazione del gestore) per adempiere al nostro provvedimento. Cercheremo in tutti i modi di arrivare all'obiettivo, ma questo non è sufficiente. Si tratta, infatti, di un caso specifico rispetto ad accessi illeciti conseguenti alla mancanza di specifiche misure a protezione dei dati di traffico.

Fin dalla programmazione 2005 ci siamo posti l'obiettivo di arrivare rapidamente al provvedimento generale che detterà le regole per la protezione di tutte le banche dati di traffico telefonico. A tal fine abbiamo già svolto sette ispezioni per 16 giorni lavorativi presso il principale gestore telefonico italiano, e una giornata ispettiva presso gli altri gestori, prevedendo anche un programma che incrementa tali attività. Ovviamente, l'enorme carico di informazioni di fronte alle quali ci siamo trovati ha rallentato la nostra attività; ad ogni modo, speriamo entro il primo semestre 2007 di varare il provvedimento per poi verificarne l'attuazione. È inutile fare grida manzoniane senza verificare la concreta attuazione delle misure adottate.

Non ci siamo interessati soltanto delle banche dati di traffico telefonico. A partire dal luglio 2005 altri fenomeni hanno fatto emergere inquietanti attività illecite di conoscenza dei dati contenuti nella più grande banca dati di sicurezza pubblica: il Centro elaborazione dati del Ministero dell'interno. D'intesa con il Ministro, il vice capo della Polizia responsabile del CED e il capo della Polizia, abbiamo avviato una attività ispettivo-collaborativa che si protrae ormai da un anno e mezzo e che ha già dato vita a quattro provvedimenti. Come è noto, uno degli accorgimenti adottati in seguito alla nostra attività collaborativa è stato quello di restringere l'accesso ai dati soltanto agli ufficiali di polizia giudiziaria,

limitando per gli agenti di polizia giudiziaria l'accesso solo ad alcuni tipi di dati. Questa è un'altra esperienza di enorme rilevanza.

Più volte abbiamo posto in essere provvedimenti di carattere generale relativi alla conservazione dei dati contenuti nell'anagrafe tributaria.

In proposito faccio presente che, in base a quanto disposto dal decreto-legge da voi convertito la scorsa settimana e a quanto sarà stabilito in sede di approvazione della finanziaria 2007, l'anagrafe tributaria procederà all'acquisizione di un maggior numero di dati. Visti però gli inquietanti fenomeni verificatisi e a tutti noti (soprattutto in considerazione della necessità di pagare le tasse, dovere costituzionale fondamentale almeno quanto la protezione dei dati), sarà ancor più necessario ed urgente porre in essere un'attività non solo ispettivo-collaborativa (termine quest'ultimo che uso per alleggerire l'espressione, ma non va dimenticato che la nostra è un'Autorità di garanzia indipendente) ma anche di verifica e controllo sull'anagrafe tributaria, al fine di garantire le misure di sicurezza necessarie a proteggere i dati sia da accessi esterni, sia da usi illegittimi da parte di soggetti interni.

Questo è lo scenario di fronte al quale siamo impegnati. Ho trattato marginalmente la libertà di informazione non perché sia meno importante, ma perché è un tema più tradizionale. Di fronte a questo scenario ribadiamo l'impegno assoluto a fare fino in fondo il nostro dovere, molto più di quanto sia prevedibile umanamente. Sappiate però che la nostra Autorità è quella che presenta l'organico più ridotto. La nostra pianta organica prevede 100 persone, il 50 per cento in meno di quella prevista per l'Autorità per l'energia elettrica e il gas, la seconda per dimensioni dopo la nostra. Le risorse umane e i mezzi per lo svolgimento dell'attività ispettiva e informatica sono eccellenti sotto il profilo della qualità professionale delle persone, ma assolutamente insufficienti dal punto di vista numerico.

Abbiamo, inoltre, poteri limitati e del tutto insufficienti soprattutto dal punto di vista sanzionatorio. Vi basti sapere che nella migliore delle ipotesi e solo per una fattispecie quasi marginale in questo panorama (la mancata notificazione al Garante del trattamento dei dati) possiamo comminare al massimo una sanzione pecuniaria di 60.000 euro, che può essere aumentata fino al triplo. Ricordo, però, che un solo nostro provvedimento ha richiesto investimenti per 30 milioni di euro. Se la sanzione che possiamo comminare arriva al massimo a 180.000 euro, siamo evidentemente privi di armi: andiamo in battaglia senza avere neanche un coltellino! Abbiamo bisogno di poteri sanzionatori maggiori, anche perché l'unico altro nostro potere è troppo forte: bloccare il trattamento dei dati. Ovviamente, il 31 dicembre non si potranno bloccare le intercettazioni legittime richieste dall'autorità giudiziaria solo perché quest'ultima non si è adeguata alle misure di protezione richieste. Allo stesso modo, non si potrà bloccare il sistema di telecomunicazioni del Paese a protezione di dati di traffico non adeguatamente tutelati. Ne consegue quindi che il blocco del trattamento dei dati è un potere troppo forte che non può essere utilizzato con la necessaria elasticità richiesta dal quadro che vi ho illustrato.

Abbiamo bisogno di maggiori risorse umane. E non è il tradizionale pianto, come dimostrano i dati difficilmente contestabili che ho citato. Abbiamo bisogno della vostra attenzione in qualità di legislatori, ai quali chiediamo non solo aiuto, ma anche di incrementare i nostri poteri sanzionatori ed aumentare le nostre capacità ispettive. In cambio vi garantiamo l'assoluta fedeltà ai nostri doveri istituzionali e la passione che anima tutto l'ufficio e il collegio, nella consapevolezza che ci si muove davvero sulla frontiera tra libertà e democrazia da un lato e controllo e paura dall'altro.

Ringrazio ancora tutti voi per l'attenzione che avete prestato e il Presidente per l'invito e le gentili parole introduttive che ha rivolto al mio indirizzo. Ovviamente, resto a vostra completa disposizione.

PRESIDENTE. Ringrazio il presidente Pizzetti per l'appassionata e travolgente relazione.

PASTORE *(FI)*. Presidente Pizzetti, la ringraziamo per la presenza, peraltro molto auspicata dalla Commissione. Anche noi ci siamo incrociati con le emergenze che, invece di affrettare questo momento, lo hanno allontanato. Si è avuta una visione piuttosto parziale delle importantissime funzioni che l'Autorità da lei presieduta svolge e ci si è concentrati su temi certamente molto «caldi» ma che, tutto sommato, rappresentano una parte abbastanza limitata delle problematiche esistenti in materia di protezione dei dati personali.

Anche se lo ha già fatto con dovizia di argomenti, vorrei ripercorrere brevemente alcune vicende da lei definite emergenziali, alcune delle quali non sono tali, ma che comunque connotano il momento politico ed istituzionale che stiamo vivendo. Il presidente Pizzetti si è intrattenuto sulla questione delle intercettazioni autorizzate, cioè lecite, fornendo indubbiamente una risposta di metodo. Verificheremo in seguito se la sostanza avrà l'esito da tutti auspicato.

Premesso che non credo che la questione competa a lei, ricordo comunque a me stesso il problema relativo al diritto di cronaca e alle notizie concernenti questioni assolutamente personali di soggetti intercettati, magari per mera casualità, nel corso di procedimenti investigativi. Tutto ciò spesso attiene a una forma di pubblicità degli stessi atti giudiziari. La questione, però, non riguarda soltanto l'aspetto relativo all'uso illegittimo dei dati personali. Non so se la Commissione giustizia abbia affrontato *ex professo* queste problematiche e quali siano stati gli orientamenti e gli eventuali interventi stabiliti al riguardo.

Presidente Pizzetti, anche la questione relativa al decreto-legge 4 luglio 2006, n. 223, ha attraversato le sue competenze e responsabilità. Come ricorderà, la cosiddetta legge Visco-Bersani ha suscitato non poche perplessità, oltre che vere e proprie critiche da parte dell'Autorità, poi ribadite nel documento fortemente sollecitato, che lei ha consegnato agli atti. La problematica posta da quel decreto-legge non soltanto si è consolidata, dal momento che non mi risulta che siano state apportate particolari modifiche legislative, ma si è accentuata a seguito dell'adozione dei suc-

cessivi provvedimenti, che pongono indubbiamente un problema di metodo. All'epoca, lei ha significato alla Commissione (ho ascoltato la sua audizione) la necessità di evitare che in un unico archivio siano concentrati milioni di dati, che potrebbero essere facilmente acquisiti da chi ha la possibilità di accedere a quell'archivio, senza quelle procedure di garanzia che, in presenza invece di una pluralità di archivi, rendono in ogni caso la sequenza dell'informazione maggiormente garantita per il soggetto interessato. Un conto è accedere agli archivi delle banche, magari interrogando un unico archivio gestito autonomamente; altro è accedere ai milioni di dati raccolti nell'anagrafe tributaria, che possono essere utilizzati anche in modo poco significativo, magari per fini diversi da quelli della lotta all'evasione tributaria.

Nel corso dell'audizione presso la Commissione parlamentare di vigilanza sull'anagrafe tributaria, il vice ministro Visco, con una simpatica *boutade* (almeno immagino sia stata tale), proprio a proposito del cosiddetto spionaggio tributario, ha creduto di rassicurare i colleghi parlamentari dichiarando che i vip avrebbero avuto un accesso più garantista di quello relativo ai comuni mortali. Naturalmente il presidente Pizzetti sa benissimo – come ha anche dichiarato – che i comuni mortali hanno bisogno di più garanzie delle persone con una certa rilevanza pubblica, beneficiando di un minore diritto alla protezione dei propri dati.

Poi vi è stata la vicenda da lei ricordata del cosiddetto spionaggio Telecom, che indubbiamente è stata molto rilevante.

Per quanto riguarda i titolari di *password* che hanno diritto ad accedere all'anagrafe tributaria, si è trattato probabilmente solo di una curiosità o almeno speriamo sia così. In ogni caso, da un lato, ci rassicura il fatto che non vi siano fenomeni di devianza rilevante; dall'altro, ci preoccupa che all'anagrafe tributaria possano accedere molte persone, anche gli impiegati di livello modesto. Pertanto, questi fenomeni potrebbero essere molto diffusi; anzi sarebbe opportuno verificare se vi sono stati fatti che non riguardano solo i cosiddetti vip, ma anche persone che tali non sono.

Vorrei anzitutto chiederle quali sono le proposte dell'*Authority* in materia di poteri sanzionatori ed interdittivi. Lei ha fatto un esempio in materia di poteri interdittivi che è di estrema rilevanza ma non credo si tratti di fenomeni globali che possano formare oggetto di divieto.

A suo parere, in che misura è ipotizzabile un intervento riguardo alla libertà di cronaca? Se sente di dare qualche suggerimento, quali «sanzioni indirette» possono essere efficaci in caso di un'eventuale violazione della *privacy* nell'esercizio del diritto di cronaca, magari con forme di pubblicazione successiva da parte dei giornali? Analoghe considerazioni valgono in materia di sanzioni pecuniarie.

Le vorrei poi rivolgere un invito. A mio giudizio, la normativa sulla tutela della *privacy* è un po' datata. Lei ha ricordato che nel 2007 decorrerà un decennio dalla istituzione dell'Autorità. Nella sua premessa ha anche precisato che in questi dieci anni vi sono stati cambiamenti molto radicali. L'impressione che ha l'opinione pubblica, ossia il cittadino comune, è che la *privacy* si sia ridotta nella sostanza ad adempimenti di ca-

rattere burocratico. Oggi infatti in qualsiasi ufficio viene subito chiesto di firmare modelli per la tutela della *privacy* (in banca, dal professionista). Nella sostanza, però, siamo nel mondo il Paese in cui la *privacy* è meno tutelata e ci si sente presi in giro.

Come ho detto, nella vita di tutti i giorni appare una distonia profonda tra quel che si vede, si sente e si legge sul trattamento dei dati, acquisiti più o meno lecitamente, e la quotidianità, in cui sembra che la tutela della *privacy* consista nel famoso modulo che si firma ai punti a), b) o c) a seconda delle autorizzazioni che il cittadino deve rilasciare a chi in quel momento entra in possesso di certi dati personali. A suo avviso, questa normativa, piuttosto farraginosa, pesante, forse nemmeno necessaria allo scopo e attuata in maniera esageratamente burocratica, può essere rivista?

Fortunatamente non è questo il problema più rilevante; ciò nonostante mi preme evidenziarlo al fine sia di ristabilire con il cittadino comune un rapporto «amichevole», sia di semplificare la vita quotidiana.

QUAGLIARIELLO *(FI)*. Presidente Pizzetti, anch'io la ringrazio per la relazione svolta. Credo – e ne sono ancor più convinto, dopo averla ascoltata – nella necessità di trovare canali di comunicazione di carattere istituzionale più forti tra il Parlamento e le *Authority*, soprattutto con quella che lei presiede. Non dobbiamo dimenticare, infatti, che il rapporto istituzionale tra il potere legislativo e questo tipo di *Authority* è preminente e, a mio avviso, per tutelarlo non basta una relazione annuale e la manifestazione che intorno ad essa si inscena. È necessario trovare strumenti più ordinari di comunicazione. Questo potrebbe essere un tema di riflessione anche per noi, in sede di Commissione.

Dalla sua relazione emerge con chiarezza come le problematiche che interessano l'Autorità da lei presieduta, dal momento in cui è stata istituita ad oggi, si siano modificate, diventando più rilevanti per quel che concerne la vita sociale e lo stesso conflitto politico. Se valuto alcune impostazioni che hanno caratterizzato la prima fase di vita dell'Autorità per la tutela della *privacy*, quando non era lei a presiederla, credo – lo lasci dire a me – di poter rilevare un diverso approccio culturale, che è confermato anche dalle sue parole odierne. Ad esempio, a cospetto di una impostazione molto più «ideologica» e basata sulla fissazione di diritti, lei ha oggi proposto la ricerca di punti di mediazione tra esigenze differenti. A mio parere, tale cambiamento non è solo frutto di scelte culturali differenti; sappiamo che al riguardo vi è un conflitto tra l'impostazione di tipo continentale e quella di tipo anglosassone, in particolare, americana. Tuttavia, al di là dell'ideologia, penso che un cambio di paradigma si sia reso obbligatorio anche, e soprattutto, per le problematiche nuove, emerse dalle vicende storiche.

Pertanto, la sua relazione è utilissima come introduzione, ma merita approfondimenti successivi, soprattutto sul tema del rapporto tra gli strumenti a disposizione dell'*Authority* e i fini di fondo che essa si prefigge. Al riguardo, vanno messi in rilievo due aspetti, il primo dei quali è che i

mezzi e gli obiettivi sono predeterminati solo in parte e dipendono, peraltro, da scelte di indirizzo politico che, come tali, non possono escludere il Parlamento. Per chiarire questo punto mi ricollegherò alle sue parole. Lei ha detto che il dovere di far pagare le tasse – e quindi la lotta all'evasione – è almeno pari a quello di tutelare i dati personali. Come affermazione astratta, può essere condivisa. Questo dovere si può però interpretare in tanti modi: adottando politiche di incoraggiamento alla contribuzione, ovvero che puntano al controllo e alla «persecuzione» dei contribuenti. In altro ambito, laddove vi è contrasto tra le esigenze di investigazione della magistratura e le libertà personali dei cittadini per quanto concerne la tutela della *privacy*, si possono operare scelte diverse o trovare punti di mediazione differenti. Tutto ciò, almeno in parte, dipende anche dalla volontà politica; proprio per questo ritengo importante il contatto tra l'*Authority* e il Parlamento.

Il secondo aspetto è relativo alla strumentazione, ai mezzi e agli strumenti di carattere giuridico a disposizione dell'*Authority* per raggiungere i suoi obiettivi. Lei ha detto, ad esempio, che di fronte alla scelta di bloccare le attività della magistratura laddove non ci si è conformati a quanto stabilito, l'Autorità deve alzare le mani. Ciò è comprensibile. Tuttavia, si renderà conto (è un suo problema che, però, è in parte anche nostro) che oggi, proprio per non aver adeguato i mezzi rispetto ai nuovi fini dell'*Authority*, sembra che si intervenga sempre in ritardo sulle situazioni: vale a dire nel momento in cui esse si sono già realizzate causando un danno non più emendabile.

Da qui deriva la dissimmetria cui ha fatto riferimento il collega Pastore. Da una parte c'è la convinzione diffusa che queste tematiche siano sempre più importanti, dall'altra si ha l'impressione, ingiusta, che la sua struttura in realtà non sia in grado di intervenire sulle nuove emergenze sociali, facendolo soltanto in una dimensione burocratica che rappresenta un aggravio per il cittadino. Riflettendo e intervenendo sul rapporto tra mezzi e fini, probabilmente questa sensazione diffusa potrebbe essere emendata.

In conclusione, le mie richieste sono due. Da una parte vorrei sapere fino a che punto condivide questo tipo di analisi; dall'altra, vorrei chiederle di tornare nuovamente in Commissione per approfondire lo specifico aspetto del rapporto, affinché attraverso una collaborazione con gli organi legislativi si possano apportare le dovute correzioni.

VILLONE *(Ulivo)*. Signor Presidente, vorrei partire dalle considerazioni svolte poc'anzi dai colleghi, giacché dagli interventi dei senatori Pastore e Quagliariello sembrerebbe quasi che con la tutela della *privacy*, svolta dall'Autorità qui rappresentata dal presidente Pizzetti, siamo di fronte ad una sorta di inutile superfetazione burocratica che, alla fine, non garantisce il risultato. Il nostro Paese è allineato all'esperienza europea, che è caratterizzata da una tutela considerevole della *privacy*. Vi sono esperienze in cui la *privacy* non gode dello stesso tipo di tutela. Il presi-

dente Pizzetti riferiva dell'attenzione costante posta in sede europea a tale argomento.

Per portare un esempio che tutti comprendono facilmente, ricordo come negli Stati Uniti la sensibilità collettiva verso il valore della *privacy* è assai meno intensa che nel nostro Paese. Non possiamo partire dalla convinzione che il nostro livello di attenzione su questo argomento è basso, giacché come sistema Paese facente parte di una più vasta esperienza, quindi su un piano comparato, possiamo dire che non è affatto così. La possibilità di tutelare effettivamente la *privacy* risente di fattori diversi e in particolare di due di essi: il contesto di emergenza, che non può essere trattato in maniera superficiale e frettolosa; il fattore tecnologico. Oggi la diffusione dei dati, non necessariamente finalizzata alla violazione della *privacy* ma semplicemente a livello di disponibilità, rappresenta un'acquisizione non reversibile del modo di essere della nostra società. Pertanto, quando un dato è acquisibile e acquisito non è pensabile assicurare elementi di tutela assoluta e imperforabile. La maggiore disponibilità di dati comporta un maggior rischio che i dati entrino in circolazione: ciò appare inevitabile.

Tuttavia, se l'evoluzione tecnologica permette di disporre più ampiamente dei dati, pensare di settorializzare queste informazioni, impedendo ad esempio alle pubbliche amministrazioni di mettere insieme un *pool* di conoscenze, perché potrebbe essere pericoloso e dar luogo ad una sorta di grande fratello, è una petizione di principio destinata a non andare molto lontano.

Pertanto, le domande che dovremmo porre al presidente Pizzetti dovrebbero essere formulate nei seguenti termini: nel contesto attuale, con le pressioni odierne, con le attuali condizioni di avanzamento tecnologico, si può ragionevolmente fare qualcosa per tutelare, nella misura maggiore possibile, il dato che si considera degno di tutela? si stanno omettendo elementi su cui si potrebbe intervenire meglio?

Non poniamoci l'impossibile obiettivo di blindare i dati rispetto ad una condizione in cui questo fine non può essere di per sé utilmente perseguito. Cerchiamo di acquisire dall'Autorità l'indicazione per interventi, utili e possibili dal punto di vista normativo e tecnologico, finalizzati a rafforzare il valore da tutelare. Non partirei però dall'idea che se alla nostra definizione di tutela diamo un valore pari a cento e arriviamo ad un risultato di 94, tale risultato sia percepito come un fallimento dell'Autorità.

SINISI *(Ulivo)*. Signor Presidente, sarò brevissimo intendendo manifestare al presidente Pizzetti, che saluto, una sola ed esclusiva preoccupazione. Basta guardare una certa filmografia per capire che il problema dei dati personali sarà in futuro uno dei temi cogenti della nostra vita di relazione e uno dei presidi della nostra libertà pubblica e privata. Basta leggere qualche manuale di filosofia per capire che la progettazione del nostro futuro passa attraverso la programmazione della sicurezza e della libertà. Credo, pertanto, che dovremmo approfondire meglio i confini del

rapporto tra sicurezza e libertà. Poiché la sicurezza può essere vista come valore strumentale per la libertà (argomento sul quale ci siamo capiti piuttosto bene, avendo chiarito i nostri orizzonti nell'ambito del dibattito fin qui svolto), ciò che a mio avviso deve essere chiaro e non può non essere deciso è che la soglia entro cui debbono muoversi gli apparati di sicurezza dello Stato deve essere più avanzata rispetto a quella garantita ai privati cittadini, in considerazione dell'esercizio funzionale della loro missione.

Qualche anno fa ho provato un certo imbarazzo nel constatare che alcune cose non consentite agli apparati di pubblica sicurezza lo erano invece a società di tipo commerciale. In sostanza, alcuni dati che non possono essere acquisiti liberamente dagli apparati di sicurezza erano acquisibili attraverso società commerciali a pagamento. Su questo punto dobbiamo intenderci per capire cosa, a chi ed entro quali limiti dobbiamo consentire l'accesso ai dati. Certamente ci orienta il principio pertinenziale, ma se vogliamo dare un valore alla funzione della sicurezza nel nostro Paese, dobbiamo garantire che essa possa essere esercitata utilizzando questi dati in maniera maggiore rispetto a quanto non sia consentito ai singoli privati cittadini. È un tema di confine.

Voglio evitare di intrattenermi sulle questioni di cronaca. Sull'altare della modernità saremo comunque chiamati a pagare un prezzo per la diffusione dei contenuti, difficilmente arginabile anche se probabilmente sanzionabile, delle intercettazioni legittimamente acquisite. Dobbiamo evitare il rischio che il Garante della *privacy* si trasformi in una sorta di autorità morale nel nostro Paese; speriamo piuttosto che svolga una funzione giuridica e tecnica entro confini precisi.

È stato fatto un accenno alla possibilità di utilizzare indebitamente le banche dati, che sono consentite e addirittura previste da istituzioni pubbliche. Al riguardo evidenzio che dobbiamo giovarci delle banche dati e non averne timore, pur preoccupandoci del modo in cui esse vengono utilizzate. Ciò probabilmente richiede una rivisitazione degli strumenti legislativi a disposizione.

Confido nella premessa che è stata svolta, cioè nella volontà di spostare l'accento delle vostre funzioni sugli apparati di controllo. In buona sostanza, per evitare di essere troppo generici, è necessario intervenire sulle singole questioni senza scandalizzarsi ed avendo a disposizione un apparato dello Stato in grado di farlo.

Alla vicenda dell'anagrafe tributaria preferisco non fare cenno, ma voglio evidenziare un aspetto positivo: è pur vero che vi sono state centinaia di accessi abusivi, fatto gravissimo, sanzionato penalmente se l'utilizzo dei dati è stato indebito. È anche vero, però, che vi sono stati strumenti informatici e di *audit* che hanno consentito di verificare tali accessi. Se è stato possibile individuare singolarmente tutti coloro che hanno avuto accesso ai dati in modo illecito, sussistono evidentemente strumenti di protezione. Ogni volta che si scopre una violazione, bisogna riflettere sul fatto che vi sono idonei strumenti che ne consentono l'individuazione. Bisogna addolorarsi del fatto che le violazioni si verificano, ma anche giovarsi della sussistenza degli strumenti di verifica e di contrasto.

CALVI *(Ulivo)*. Signor Presidente, rispetterò il suo invito alla brevità e mi limiterò a svolgere soltanto alcune osservazioni.

Contrariamente a quanto ho ascoltato, almeno negli interventi dei senatori Quagliariello e Pastore, non condivido in alcun modo quanto è stato evidenziato e che, a mio avviso, deriva da una carenza di informazioni e da una non perfetta conoscenza delle funzioni dell'ufficio del presidente Pizzetti e delle norme che regolano il Garante della *privacy*. In sostanza, si è affermato che siamo di fronte ad uno strumento di opinabile utilità perché in qualche modo «arriva dopo»: lo stesso giudizio, allora, potrebbe essere espresso nei confronti della magistratura, che ovviamente agisce *a posteriori*. Considero questa osservazione un po' stravagante e non appropriata.

Credo piuttosto che il problema reale non riguardi l'*Authority* ma il Parlamento. Francamente, se dovessi esprimere un giudizio – che ovviamente non mi spetta – e se dovessi fare una valutazione, sia pure generica, sottolineerei che il lavoro svolto dal Garante della *privacy* ora e nella precedente gestione è ammirevole, apprezzabile e valutabile in modo straordinariamente positivo. Con le decisioni dell'Autorità è stata introdotta una cultura di garanzia come raramente è stato visto nelle sentenze e nella legislazione. Ribadisco, dunque, che il vero problema riguarda il Parlamento proprio perché non è riuscito né a conferire poteri adeguati né ad individuare gli ambiti normativamente scoperti.

Sarò molto sintetico ed affronterò soltanto il problema delle intercettazioni telefoniche. È inutile parlare di quelle illecite, delle quali – proprio perché illecite – si occuperà il giudice penale. Il Parlamento, invece, ha il dovere di riflettere e di interessarsi dell'uso indebito delle intercettazioni lecite. Questo problema, infatti, riguarda lei ma innanzi il Parlamento.

Ci troviamo di fronte a due interessi contrapposti ma costituzionalmente garantiti: la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, come recita l'articolo 15 della nostra Carta costituzionale. Nello stesso tempo, vi è il dovere di intervenire e prevenire ogni forma di delinquenza e criminalità organizzata. La nostra legislazione ha oggi trovato un equilibrio che però non è più sufficiente e non garantisce. Si è stabilito che solo per i reati per i quali è prevista una pena superiore ai 5 anni è ammissibile ed autorizzabile un'intercettazione richiesta dal pubblico ministero. Pur tuttavia abbiamo assistito ad un eccesso di autorizzazioni. Come sappiamo, la grande mole di autorizzazioni ha creato preoccupazioni anche sul piano strettamente economico. Ritengo, però, che in proposito il legislatore non possa intervenire.

Non bisogna dimenticare che nel nostro Paese vi sono strutture di criminalità organizzata straordinariamente feroci e che vi sono stati momenti in cui ben cinque Regioni italiane sono state nelle mani della *'ndrangheta*, della mafia, della camorra, della stidda e della sacra corona unita. La diffusione della criminalità organizzata è stata tale che non si è potuto in alcun modo chiedere l'attenuazione o privare la magistratura del fondamentale strumento delle intercettazioni.

Il problema si manifesta però nell'uso indebito dell'intercettazione lecita, vale a dire in una fase successiva. Su questo punto il Parlamento è in gravissimo ritardo e il decreto-legge 22 settembre 2006, n. 259, recentemente approvato con l'accordo di tutti, è totalmente inefficace. Oggi sappiamo che non ci sono intercettazioni illecite e che non possiamo cancellare nulla. Si pone invece il problema di verificare, una volta effettuata un'intercettazione lecita, l'uso e l'ostensibilità della sua diffusione.

Abbiamo osservato spesso la tecnica con cui opera la magistratura: l'intercettazione è immessa all'interno di un atto giudiziario che viene depositato. A questo punto viene meno lo sbarramento della segretezza e l'atto viene riportato su tutti i giornali, anche quando non è assolutamente utile ai fini dell'indagine. Paradossalmente, l'intercettazione che avrebbe dovuto essere finalizzata a scoprire una traccia di un reato, o comunque ad intervenire perché esso non fosse portato a ulteriori conseguenze, diventa uno strumento creatore di nuove fattispecie. Cito un esempio noto, forse il più banale, ma proprio per questo il più grave: il giornale che pubblicò l'intercettazione di una comunicazione tra una nota attrice e un noto finanziere, in cui la moglie diceva al marito «ti voglio bene». Mi domando ancora quale necessità vi fosse – attenzione! – non di intercettare, ma di rendere pubblica quella intercettazione attraverso il deposito in un atto e poi, sgombrato il terreno dalla segretezza, attraverso la pubblicazione su un giornale. In questi casi l'intervento dell'Autorità è veramente fondamentale, perché spetta a lei censurare. Ma prima dell'intervento del Garante, è compito del Parlamento impedire che si verifichino situazioni quale quella indicata. Sono stati presentati vari disegni di legge che regolamentano proprio questa fase successiva. Personalmente, ho presentato un disegno di legge addirittura nella XIII Legislatura.

Vi sono stati conflitti politici intorno a questo tema. Il problema non è limitare l'uso dell'intercettazione, non potendosi stabilire *a priori* cosa diranno taluni soggetti quando si può pensare che in quell'area si stanno magari organizzando crimini, come abbiamo visto. È giusto che non vi sia alcuna limitazione, se non appunto quella della pena massima non inferiore a cinque anni per poter intercettare.

Il problema è quale uso si farà delle intercettazioni. In materia non esistono norme. Il nostro codice penale, con gli articoli da 266 a 271, regolamenta in modo molto preciso e garantistico la fase anteriore, tanto che non toccherei nulla dell'impianto normativo. Di contro, non vi è regolazione della fase successiva: non si stabilisce chi sia il responsabile della custodia (io l'ho individuato nel pubblico ministero), né quale parte dell'intercettazione debba essere distrutta. Non è detto che in un processo vada distrutta tutta la parte non utile all'accusa, dal momento che vi può essere una intercettazione straordinariamente utile anche alla difesa. Si tratta di una materia molto precisa, su cui ho molto riflettuto e il disegno di legge che ho presentato cerca di regolamentare questa fase.

Siamo su un terreno di grande delicatezza, in cui le garanzie fondamentali del cittadino, che sono quelle indicate dall'articolo 15 della nostra Carta costituzionale, devono trovare un equilibrio ragionevole con l'ovvia

e naturale esigenza di impedire che la sicurezza sia turbata da organizzazioni criminose quali quelle che operano sul nostro territorio. In tal senso, la vostra giurisprudenza è di rilevante interesse. Citerò solo un esempio che ho molto apprezzato e che riguarda il vostro recente intervento a proposito di una nota trasmissione televisiva: l'intero Parlamento si stava piegando con interventi sconsiderati; alcuni si erano, addirittura, offerti di fare quell'esperimento, mostrando una qualità intellettuale non particolarmente apprezzabile. Ebbene, la vostra decisione è stata veramente esemplare, per la qualità culturale che è stata riversata in essa e per la capacità di intervenire subito e garantire tutti e non alcuni.

Portando la collaborazione tra voi e noi sul terreno dell'individuazione di interventi normativi doverosi da parte del Parlamento per aiutare il vostro lavoro di controllo, si potrebbe lavorare insieme e cooperare per trovare soluzioni normative equilibrate e ragionevoli, tutelando i diritti dei cittadini con riferimento sia alla segretezza e alla *privacy* sia alla sicurezza.

PRESIDENTE. La quantità e la qualità delle domande formulate evidenziano il vivo interesse della Commissione, certamente sollecitato dall'ampiezza della relazione del presidente Pizzetti, che ringrazio nuovamente.

Rinvio il seguito dell'audizione del Presidente dell'Autorità garante per la protezione dei dati personali e il seguito della indagine conoscitiva ad altra seduta.

I lavori terminano alle ore 18,25.

€ 1,00