



Giunte e Commissioni

**RESOCONTO STENOGRAFICO**

n. 2

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

**1<sup>a</sup> 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**

60<sup>a</sup> seduta: mercoledì 13 dicembre 2006

Presidenza del presidente BIANCO

## I N D I C E

## Seguito dell'audizione del Presidente dell'Autorità garante per la protezione dei dati personali

PRESIDENTE . . . . .	Pag. 3, 13, 19	* PIZZETTI . . . . .	Pag. 3, 14
VILLONE ( <i>Ulivo</i> ) . . . . .	13		

---

**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 Democratici cristiani 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 professor Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali, accompagnato dal segretario generale Giovanni Buttarelli, nonché da Mario de Bernart, Baldo Meo, Laura Tempestini e Alberto Corsini.*

*I lavori hanno inizio alle ore 14,35.*

*PROCEDURE INFORMATIVE*

**Seguito dell'audizione del Presidente dell'Autorità garante per la protezione dei dati personali**

PRESIDENTE. L'ordine del giorno reca il seguito dell'indagine conoscitiva sui rapporti tra libertà d'informazione, sviluppo delle comunicazioni, tutela dei diritti della persona e sicurezza pubblica, sospesa nella seduta del 29 novembre scorso.

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 il seguito dell'audizione del professor Francesco Pizzetti, presidente dell'Autorità garante per la protezione dei dati personali, qui presente con alcuni suoi collaboratori, che saluto e ringrazio per essere di nuovo fra noi. Ricordo che il professor Pizzetti nella precedente seduta aveva svolto il suo intervento e che alcuni colleghi avevano posto delle domande. Cedo quindi la parola al nostro ospite, ringraziandolo sin d'ora per le risposte e i chiarimenti che vorrà cortesemente fornire alla Commissione.

*PIZZETTI.* Ringrazio in primo luogo il Presidente e la Commissione per l'opportunità che ci viene offerta di intervenire nuovamente in questa sede al fine di completare l'audizione e quindi fornire le risposte ai quesiti che sono stati posti nella scorsa occasione, rimanendo ovviamente a disposizione per ogni ulteriore approfondimento che i senatori ritenessero necessario. Cercherò di rispondere il più puntualmente possibile alle diverse domande che sono state poste, in alcuni casi accorpandole quando i quesiti dei senatori affrontano problematiche tra loro affini.

Il primo intervento era stato del senatore Pastore, che ringrazio per la sua cortesia, ed aveva toccato una serie di aspetti. Il primo riguardava il difficile rapporto tra diritto di cronaca e riservatezza, come tema generale, e poi la tematica, che negli ultimi mesi ci ha purtroppo coinvolto nume-

rose volte, relativa alla pubblicazione del contenuto di intercettazioni telefoniche, nella maggior parte dei casi legittimamente disposte dalla autorità giudiziaria, secondo il codice di procedura penale, per finalità di giustizia, e che poi sono state pubblicate sui giornali.

Analoga questione è stata oggetto di una domanda posta dal senatore Calvi, anche in riferimento specifico ai disegni di legge presentati in materia dallo stesso senatore Calvi e dal Governo. Ovviamente, svolgerò considerazioni che abbiamo già avuto modo di richiamare altre volte, ma ritengo che sia proficuo farlo in questa sede onde poter approfondire con voi questa problematica.

L'Autorità, per la sua responsabilità e per le competenze che il legislatore le ha attribuito in questa materia, è coinvolta nel difficilissimo compito di trovare il corretto equilibrio tra diritto di cronaca, diritto alla riservatezza e diritto alla protezione dei dati personali: in questo caso si tratta più frequentemente della violazione del diritto alla riservatezza e della tutela della dignità personale. Per ragioni di tempo non mi soffermerò su questo argomento, tuttavia tengo a precisare che, come è noto, questo è proprio l'aspetto che dà vita per la prima volta nel dibattito culturale e nell'esperienza giuridica alla «costruzione» del diritto alla *privacy*.

Il *right of privacy* nasce proprio nella Boston di fine Ottocento di fronte al problema della pubblicazione sulla stampa bostoniana di notizie relative ai comportamenti di una cittadina americana, la signora Warren, nella sua vita sociale. Si tratta di un tema classico della nostra materia, che nel caso italiano è accentuato dall'ampiezza delle competenze riconosciute al Garante ed anche dalla rilevanza che nel codice della *privacy* è attribuita a questa tematica. Vi sono due diritti che hanno valore costituzionale; mi riferisco, da una parte, al diritto di cronaca e di informazione, ovvero il diritto ad essere informati, che è un fondamento della democrazia, e, dall'altra, alla tutela della riservatezza, che è un compito specifico della nostra Autorità, ma soprattutto un diritto fondamentale riconosciuto come tale dalla normativa europea, ed oggi anche dalla Carta dei diritti dell'Unione europea.

La linea che in questo ambito abbiamo sempre seguito è stata quella di sottolineare che per le persone pubbliche, che devono rendere conto all'opinione pubblica dei propri comportamenti secondo modalità più incisive di quanto non avvenga per i normali cittadini, il diritto alla riservatezza è affievolito. Infatti, in molti casi prevale il diritto dell'opinione pubblica ad essere informata per poter esercitare il proprio giudizio, conoscere e valutare. Parallelamente, tuttavia, abbiamo anche sempre ribadito che il diritto alla riservatezza non è comprimibile senza limiti anche nei confronti delle persone pubbliche, posto che va sempre tutelata la dignità delle persone e rispettato il principio di non acquisire informazioni o notizie con artifici, raggiri o modalità che incidano, appunto, sulla sfera più intima della libertà personale e dell'attività di ciascuno.

Per quanto riguarda la pubblicazione delle intercettazioni, abbiamo ribadito in ogni contesto che le intercettazioni disposte dall'autorità giudi-

ziaria rappresentano uno strumento di attività investigativa che il nostro codice prevede. È noto che in Italia il numero delle intercettazioni telefoniche disposte dalla magistratura è molto elevato; tuttavia tengo come sempre a sottolineare che non tocca a noi giudicare se tali intercettazioni siano troppe o troppo poche, posto che valutazioni di questo tipo rientrano nella specifica competenza del legislatore in termini generali e dei singoli giudici quando fanno ricorso a questo strumento investigativo che il nostro ordinamento prevede.

Tocca invece al Garante ribadire due principi fondamentali. Mi riferisco in primo luogo al fatto che l'autorità giudiziaria ha il dovere di proteggere i dati dei cittadini di cui viene a conoscenza per fini di giustizia; non cesseremo mai di sottolineare questo profilo ed obbligo, proprio perché riteniamo che anche i giudici abbiano questo specifico dovere. In secondo luogo, la pubblicazione del contenuto delle intercettazioni, anche quando legittimamente conosciute dal giornalista o dall'operatore degli organi di informazione, deve sempre rispondere ai principi già richiamati. Ne consegue che se si tratta di persone private, va dato rilievo significativo ed esercitata particolare tutela al diritto alla riservatezza, e quindi vige il divieto di ledere la dignità personale e di dare informazioni che non siano necessarie o essenziali ai fini della conoscenza di un fatto da parte dell'opinione pubblica. Tuttavia, anche nel caso di persone che hanno un'esposizione pubblica, va comunque tenuto presente quanto richiamato.

Aggiungo che più volte abbiamo dovuto ricordare che va salvaguardata in ogni caso la figura del terzo incolpevole; frequentemente nelle intercettazioni telefoniche sono infatti coinvolte persone che non hanno alcuna «rilevanza» investigativa e spesso il contenuto delle stesse può danneggiare i familiari dell'intercettato, oppure minori, e può riguardare anche persone assolutamente incolpevoli. Il nostro richiamo è quindi sempre finalizzato a rammentare tutti questi principi. Faccio presente che ormai frequentemente, ed anche di recente, ci è capitato di dover richiamare un ulteriore profilo, posto che talvolta pubblicare il contenuto di una intercettazione significa anche rendere due volte vittima chi è già vittima di un reato. Infatti, se l'intercettazione costituisce di per sé elemento o indizio di un reato, pubblicare il contenuto delle intercettazioni in realtà significa colpire due volte la persona oggetto della telefonata: da un lato, perché si evidenzia che essa è vittima di un tentativo di reato o di un reato vero e proprio, dall'altro, perché si diffondono informazioni che sono proprio quelle che hanno costituito un elemento rilevante del reato medesimo.

Ovviamente, se ci chiedete – cosa più che ragionevole – quali sono le misure che possiamo adottare, non posso che lamentare la limitatezza delle nostre competenze. È noto che abbiamo un potere molto importante, ma che ha un effetto oggettivamente limitato, cioè quello di dichiarare, se la persona interessata ricorre a noi, l'illiceità del trattamento. Come è noto, però, non abbiamo (ed è giusto che non ci sia stato riconosciuto) il potere di stabilire il risarcimento del danno, che rimane competenza specifica dell'autorità giudiziaria; pertanto, il nostro provvedimento, pur par-

ticolarmente importante, che può essere fatto valere con molta persuasività davanti al giudice civile, ha comunque un effetto limitato per la persona interessata.

Abbiamo poi un potere devastante, una sorta di arma atomica, rappresentato dal blocco del trattamento del dato, dal divieto di pubblicazione, o di reiterazione della pubblicazione, della notizia. Tale potere viene da noi utilizzato spesso (anche quest'anno ne è stato fatto uso in più casi), ma in molte situazioni si dimostra non particolarmente adatto in quanto determina un effetto inibitorio dell'informazione stessa. Nel nostro sistema la stampa non è sottoposta ad autorizzazione o a censura. È vero che il blocco del trattamento dei dati non è propriamente un intervento censorio, ma è certamente un intervento che, determinando il divieto di pubblicazione, ha una particolare incisività. Questo è uno dei motivi per cui abbiamo chiesto al Parlamento (richiesta che ribadisco anche in questa occasione) di attribuire al Garante poteri sanzionatori più incisivi, soprattutto in termini di sanzioni pecuniarie, o uno spettro più ampio di misure sanzionatorie che ci consenta interventi più mirati ed idonei a tutelare quel bene inestimabile rappresentato dal corretto punto di equilibrio tra diritto all'informazione e tutela della riservatezza dei cittadini.

Il senatore Calvi ci ha chiesto un parere anche sul fatto che i giudici non siano più tenuti – come oggi avviene – a versare in cancelleria il contenuto delle intercettazioni telefoniche che intendono utilizzare come mezzi a supporto delle richieste di rinvio a giudizio. La domanda è suggestiva, ma per l'Autorità vale quanto ho già detto: non tocca a noi come Autorità esprimere un giudizio sulle varie modalità con le quali si può porre rimedio a questo aspetto particolarmente delicato del nostro codice di rito; infatti, esso rende difficile anche per l'autorità giudiziaria, al termine dell'attività investigativa, tutelare la riservatezza del contenuto delle intercettazioni. Nei disegni di legge presentati in questi anni (quello del Governo, quello del senatore Calvi ed anche altri) si prospettano soluzioni che, a nostro giudizio, sono di notevole interesse e meritano la massima attenzione. Ribadisco però che questa è una competenza del legislatore.

Il senatore Pastore ci ha chiesto poi di svolgere una riflessione sulle osservazioni che abbiamo avuto modo di illustrare nel corso di una audizione informale agli Uffici di Presidenza delle Commissioni riunite bilancio e finanze del Senato in sede di discussione del decreto-legge n. 223 del 2006, ma che non sono state raccolte, se non in una misura alquanto limitata. Ovviamente non possiamo che dolerci del fatto che i rilievi che abbiamo ritenuto di sottoporre all'attenzione del Senato non siano stati valutati ed accolti; in ogni caso, il legislatore non può incontrare nei provvedimenti e nelle indicazioni dell'Autorità un limite – ci mancherebbe altro! – al suo potere di legiferare. Pertanto, abbiamo preso atto di quanto contenuto nella legge di conversione. Inoltre, come abbiamo più volte affermato, una parte significativa delle regole per la tutela dei dati personali può essere oggetto di un'attenta e prudente valutazione, che noi ci aspettiamo sia fatta con la massima attenzione, in sede di attuazione della legge di conversione, quando l'Agenzia delle entrate dovrà adottare i provvedi-

menti regolatori previsti. Sul piano in cui invece il nostro potere ha un'incisività assai più rilevante, non mancheremo di prestare la massima attenzione.

Ci è stata chiesta – e così rispondo anche ad altri interventi che hanno toccato punti analoghi – la nostra opinione rispetto ai significativi illeciti negli accessi ai dati dell'Anagrafe tributaria, di cui anche noi abbiamo preso atto, sostanzialmente, attraverso i mezzi di stampa e di informazione. Ripeto che noi non siamo stati destinatari di specifici ricorsi e, quindi, non abbiamo avuto la possibilità di acquisire informazioni nell'ambito di una specifica attività ispettiva in merito a tali accessi illeciti. Anche in questo caso ribadiamo le considerazioni che l'Autorità non si stancherà mai di ripetere: è importante evitare di acquisire dati già acquisibili o conoscibili con l'accesso ad altre banche dati nelle quali questi stessi dati sono istituzionalmente contenuti. Consideriamo pertanto pregiudizievole, e sempre con sfavore, il fatto di moltiplicare le sedi di raccolta e conservazione dei dati. Dunque, anche rispetto ad alcune normative innovative in materia di Anagrafe tributaria, guardiamo con perplessità all'acquisizione nell'Anagrafe tributaria di dati conoscibili e già conservati in altre banche dati; siamo però ancora una volta in presenza di decisioni assunte dal legislatore.

Vogliamo tuttavia ribadire anche in questa sede l'assoluta necessità – sulla quale tornerò ancora – di garantire: che le banche dati siano protette; che i dati contenuti nelle banche dati per finalità previste e consentite dal legislatore siano protetti da accessi illeciti; che chi è titolare di una banca dati assicuri tutte le misure idonee ad evitare, nei limiti del possibile, del conoscibile e del prevedibile, accessi illeciti, sapendo che maggiore è la quantità di dati registrati nella banca dati, più la pericolosità dell'accesso illecito ai dati aumenta. In questo caso, leggendo le informazioni fornite dalla stampa, ma non smentite, o valutando le dichiarazioni espresse dal Ministro competente nelle sedi parlamentari, ci sembra di dover richiamare l'attenzione su un fenomeno che abbiamo già visto verificarsi rispetto ad altre banche dati. Mi riferisco alla necessità di proteggere le banche dati da accessi illeciti interni, cioè operati da soggetti che hanno titolo e diritto ad accedere ai dati solo per finalità istituzionali e che, invece, utilizzano tale possibilità per finalità diverse ed illecite.

Da questo punto di vista, pertanto, operiamo ed opereremo per accrescere le misure di sicurezza, anche con la restrizione e la compartimentazione, oltre che con la tracciabilità, dei soggetti che hanno accesso ai dati. Chiediamo con particolare incisività che da ora in avanti siano adottati strumenti di verifica preventiva sugli accessi, al fine di monitorare, o comunque individuare più facilmente, accessi illeciti prima che intervenga l'autorità giudiziaria, la quale può agire rispetto a singole fattispecie, mentre a noi interessa una protezione diffusa e generalizzata anche a carattere preventivo.

Segnalo in questo senso che abbiamo acquisito un'importante esperienza dopo più di un anno di attività collaborativa con il Centro elaborazione dati (CED) del Ministero dell'interno: come sapete, si tratta della

più grande banca dati di sicurezza esistente nel nostro Paese, alla quale accedono le Forze di polizia e di sicurezza (è cioè una banca interforze). Nell'ultimo anno e mezzo abbiamo concordato, nell'ambito di un'attività collaborativa, la selettività dell'accesso ai dati contenuti in questa banca. Abbiamo avuto anche segnali positivi circa l'introduzione di adeguati sistemi di verifica preventiva di accessi anomali che possono far pensare ad accessi illeciti.

Cercheremo di fare la stessa cosa con l'Agenzia delle entrate, con l'Anagrafe tributaria e con la società che gestisce le sue informazioni. Abbiamo instaurato un tavolo tecnico con l'Agenzia delle entrate attorno al quale si sta sviluppando un'importante attività di dialogo e di collaborazione. Pur svolgendo un'attività indipendente, riteniamo di far parte di un sistema che ha il compito di assicurare un sistema di tutela all'intero ordinamento italiano. Quindi siamo chiamati a prescrivere, a sanzionare, ma anche a collaborare. Mi pare che questo tavolo tecnico stia lavorando bene. In calendario è prevista un'attività di monitoraggio dell'Anagrafe tributaria, che definiremo meglio in seguito, compatibilmente con la disponibilità di risorse umane e mezzi. A tal fine sarà necessario stabilire uno stretto contatto con questo organismo per verificare, attraverso un'attività ispettiva e collaborativa, le modalità di conservazione dei dati e i sistemi di protezione, come facciamo da più di un anno con il CED del Ministero dell'interno.

Il senatore Pastore ci chiedeva un'opinione sulla potestà sanzionatoria nei confronti dell'attività giornalistica. Ho già espresso la mia convinzione circa l'importanza di avere un più ampio spettro di potere sanzionatorio, anche di carattere amministrativo. Nel disegno di legge d'iniziativa del Governo è contenuta una norma, alla quale guardiamo con interesse, che amplia il potere sanzionatorio dell'Autorità.

Il senatore Pastore, insieme ad altri, chiedeva poi se abbiamo la sensazione che vi sia una visione eccessivamente burocratica della nostra attività. Per quanto riguarda me e i miei colleghi, si tratta senz'altro di una preoccupazione molto forte. Se c'è una frase che più di ogni altra mi preoccupa e mi fa riflettere è proprio: «Metta qui una firma per la *privacy*». In tal modo, infatti, con un adempimento burocratico si dà conto di un'informativa che in realtà non si è avuta, perché ci si è limitati ad apporre una firma in calce ad un modulo lungo e spesso illeggibile, che costituisce una prova dell'informazione data da un punto di vista giuridico, ma non da un punto di vista sostanziale. Ciò si traduce nei confronti del cittadino in una tutela inadeguata e nella sensazione di un fatto puramente burocratico. Questo ci preoccupa molto perché l'attività da noi svolta è tutto meno che burocratica, trattandosi di difendere nella sostanza un diritto effettivo. La protezione dei dati personali dei cittadini italiani, come di tutti i cittadini, è un'esigenza crescente man mano che la nostra società si sviluppa anche mediante le moderne tecnologie.

Altri senatori ci hanno chiesto se siamo consapevoli della necessità di incrementare la protezione dei dati personali a seguito dei progressi delle tecnologie. La mia risposta è che siamo perfettamente consapevoli del



fatto che man mano che la società telematica si sviluppa e i dati corrono attraverso le reti si verificano diversi effetti. Il primo di questi è che si moltiplicano il numero dei dati dei cittadini trattati e le relative opportunità, nonchè i rischi (possiamo pagare un pieno di benzina negli Stati Uniti con un pezzettino di plastica). Il secondo effetto è che questi dati si smaterializzano. Fino a qualche anno fa il dato era contenuto in un oggetto (una cartolina, una lettera, un archivio, anche automatizzato, ma contenente comunque una serie di schede cartacee), oggi l'innovazione rilevante è la smaterializzazione del dato. È possibile inviare un'impronta digitale attraverso una sequenza alfanumerica utilizzando il sistema delle reti, che corre da una parte all'altra del mondo smaterializzando il dato. Ciò ovviamente moltiplica i rischi perché quel dato, in mancanza di un sistema di protezione efficiente, può essere conosciuto e rubato da un numero indeterminato di soggetti che hanno accesso alla rete e dispongono delle conoscenze tecnologiche adeguate, rendendo così sempre meno possibile per i cittadini autotutelarsi.

C'è pertanto un rilevante aumento del ruolo delle Autorità, che sempre più devono sviluppare non soltanto la capacità di tutelare i diritti del singolo cittadino leso, ma anche la capacità di tutelare il sistema nel suo complesso, nella consapevolezza che le modalità attraverso le quali i dati circolano (dati prima materiali, oggi smaterializzati, che prima correvano da punto a punto e che oggi corrono attraverso un sistema reticolare, moltiplicandosi i punti di accesso alla rete) richiedono un'attività particolarmente incisiva e capillare. Questo è uno dei motivi per cui credo che alla nostra Autorità si richieda sempre più una eccezionale capacità di comprensione dei fenomeni e delle innovazioni tecnologiche ed è anche una delle ragioni per cui questa Autorità è destinata, nella società presente e futura, ad operare sempre più in una zona di frontiera tra libertà e sicurezza, fra controllo e libertà.

Il senatore Quagliariello ha posto una domanda che merita una particolare attenzione. Egli ha chiesto se riteniamo adeguata la relazione annuale come modalità istituzionale di raccordo tra la nostra Autorità, che è indipendente e tale deve rimanere, e il Parlamento, che per Costituzione rappresenta il popolo italiano. Non ho alcuna difficoltà ad affermare che questo è uno strumento insufficiente, sebbene importante e irrinunciabile. Sentiamo tutti – la nostra come anche le altre Autorità – il bisogno di sviluppare ulteriori forme di raccordo, anche più frequente, con il legislatore. Uno specifico compito della nostra Autorità, che ci deriva da una direttiva europea, è il dovere di segnalare al Parlamento l'opportunità di interventi normativi a tutela dei diritti fondamentali dei cittadini. Già nella legislatura precedente i Presidenti del Senato e della Camera avevano inviato una lettera a tutte le Autorità, quindi anche alla nostra, per rimarcare tale forma di raccordo istituzionale, alla quale abbiamo risposto con interesse e assicurando la più ampia collaborazione.

Esiste già oggi una proficua attività di raccordo con il Parlamento. Ho ricordato poc'anzi la nostra audizione informale in sede di Commissioni bilancio e finanze del Senato, quindi la memoria ad esse consegnata

in quella sede. Ci sono stati altri casi in cui abbiamo avuto modo di istituzionalizzare il rapporto con le Commissioni parlamentari. Tradizionalmente intratteniamo un rapporto con le Commissioni giustizia di entrambi i rami del Parlamento, tant'è che anche nell'ambito della presente legislatura abbiamo già avuto l'onore e la fortuna di ricevere attenzione dalle suddette Commissioni proprio riguardo alle tematiche che stiamo oggi trattando, anche se, ovviamente, sotto il profilo del rapporto con l'attività giurisdizionale.

È mia opinione, condivisa dai colleghi e dai collaboratori dell'Autorità, che la Commissione affari costituzionali costituisca una sede importante per tutte le Autorità. D'altra parte, in un sistema che non prevede una Commissione *ad hoc* competente in questa specifica materia, credo che la vostra Commissione rappresenti istituzionalmente un luogo strategico delle due Assemblee parlamentari dove approfondire tutti gli aspetti che riguardano le Autorità.

Ciò è particolarmente vero per l'Autorità garante per la protezione dei dati personali, appunto, perché l'ampiezza dei settori che siamo chiamati a presidiare, l'accrescersi dei nostri compiti e lo sviluppo della società telematica richiedono sempre di più di individuare una sede istituzionale di raccordo. Ovviamente non tocca a noi – ci mancherebbe – andare oltre da questo punto di vista; ringrazio tuttavia il Presidente e tutti i membri di questa Commissione per la presente audizione, che spero costituisca l'inizio di una attività che auspico possa continuare, ovviamente compatibilmente con le vostre esigenze e disponibilità di tempo. Così come ribadisco l'importanza che ha sempre rappresentato per noi il raccordo con le Commissioni giustizia di Camera e Senato, che per molti aspetti costituiscono anch'esse una sede istituzionale molto importante, tenuto conto che la nostra Autorità è chiamata alla tutela di un diritto fondamentale dei cittadini e che rispetto all'attività giurisdizionale abbiamo molti punti di contatto, anche se ovviamente il Garante non è un'autorità giudiziaria.

Il senatore Quagliariello ha chiesto anche se riteniamo opportuno che il Parlamento ci fornisca indirizzi ed indicazioni. Ebbene, mi permetto di dire che questa ipotesi andrebbe forse troppo oltre, posto che siamo un'Autorità indipendente, che tale deve rimanere anche rispetto al legislatore. Credo però che la nostra piena disponibilità al dialogo ed a sottoporci al giudizio ed alla valutazione del Parlamento ogni qualvolta lo si ritenga opportuno – lo consideriamo un onore – e ad accogliere le indicazioni che esso ritenga di fornire, possa utilmente contribuire a realizzare un proficuo raccordo con il Parlamento, senza per questo costruire teoricamente un potere di indirizzo che forse potrebbe risultare eccessivo anche rispetto alle direttive europee.

Aggiungo che per l'Autorità garante per la protezione dei dati personali risultano particolarmente naturali il massimo rispetto e la massima attenzione nei confronti del Parlamento, dal momento che, come è noto, siamo un'Autorità interamente di nomina parlamentare, tant'è che dei quattro membri che la compongono due sono stati eletti dalla Camera e

due dal Senato, e di conseguenza l'intero organo collegiale ha una legittimazione che deriva immediatamente dalle Assemblee parlamentari. Ne consegue che, se c'è un'Autorità tenuta ad essere attentissima al rapporto con il Parlamento, questa è proprio la nostra.

Quanto alla questione del rischio di essere percepiti come un fenomeno burocratico, sollevato dal senatore Quagliariello, ho già espresso le mie considerazioni.

Dal senatore Quagliariello, ma anche da parte dei senatori Sinisi e Pastore, ci è stata chiesta la nostra opinione circa l'utilità di eventuali modifiche legislative finalizzate a dare all'Autorità un ruolo più significativo, ed inoltre se si avvertano da parte nostra nuove esigenze in ordine a poteri o competenze a cui non sia possibile dare risposta sulla base della legislazione vigente. La risposta a questa domanda è ovviamente affermativa, ed anche in questo caso vale quanto detto a proposito della nostra preoccupazione che la *privacy* sia percepita come un fenomeno prevalentemente burocratico, preoccupazione che si traduce in un vero e proprio senso di colpa quando non riusciamo a spiegare l'effetto sostanziale della nostra attività. Abbiamo l'assoluta necessità che il Parlamento ci aiuti a condurre una riflessione per adeguare la normativa che ci riguarda ai nuovi problemi che si delineano ed ai fenomeni manifestatisi nei due ultimi terribili anni che il nostro Paese ha attraversato relativamente alla protezione dei dati, nei quali si sono registrati furti di dati, attività di «dossieraggio» e spionaggio e illecite diffusioni di informazioni sui cittadini.

A fronte di tutto ciò, avvertiamo soprattutto l'esigenza di disporre di un apparato sanzionatorio più significativo; è necessario che siano ampliate le sanzioni amministrative a nostra disposizione e la fattispecie a cui applicarle. Oggi infatti le sanzioni di cui disponiamo, nel minimo e nel massimo, comportano misure pecuniarie sostanzialmente significative rispetto al singolo trattamento di dati effettuato da un cittadino nei confronti di un altro, ovvero rispetto all'illecito operato da un cittadino nei confronti di un altro cittadino, quindi nel caso di «piccoli soggetti», ma che risultano del tutto irrisorie rispetto ai fenomeni di illecito trattamento di dati operato da «grandi soggetti» come, ad esempio, quelli che gestiscono grandi banche dati. È assolutamente necessario, perciò, un incremento dei minimi e dei massimi delle sanzioni già previste dal codice.

Vi è altresì l'esigenza di individuare specifiche sanzioni amministrative per tutta una serie di violazioni relative a norme del codice della *privacy* che oggi non sono invece sanzionate, nonostante in molti casi si tratti di illeciti particolarmente delicati. Da questo punto di vista sarebbe opportuno definire adeguate fattispecie sanzionatorie riferite sia all'obbligo di vigilanza e controllo sulle banche dati, che allo stato è un obbligo generico e non specificato, sia, soprattutto, all'accertamento della violazione delle misure di sicurezza, che oggi è accompagnato da misure sanzionatorie insufficienti.

Abbiamo dunque la necessità, almeno per le grandi banche dati di rilievo nazionale, pubbliche e private, di disporre di nuove fattispecie nell'ambito sia dei poteri di controllo e vigilanza che devono essere meglio

tipizzati, sia delle sanzioni che possono essere comminate. Capite bene che di fronte all'illecito trattamento dei dati e alla mancanza di adeguate misure di sicurezza di una grande banca dati strategica per il Paese, le misure attuali, che al massimo prevedono sanzioni da 100.000 a 150.000 euro, risultano assolutamente irrisorie.

Peraltro, quando parlo di misure sanzionatorie specifiche e di fattispecie più definite in materia di controllo e vigilanza delle grandi banche dati, mi riferisco anche alla necessità di individuare quali di queste grandi strutture abbiano un significato ed una rilevanza strategica per il Paese. A questo proposito non mi stanco mai di sottolineare – e lo faccio anche in questa sede – la necessità che i Ministri della giustizia e dell'interno adottino finalmente i decreti che il codice prevede, indicando le banche dati esistenti nel Paese a fini di giustizia e di sicurezza. In assenza di questi decreti, la tutela che oggettivamente possiamo assicurare non è adeguata alle necessità, posto che non siamo in grado di conoscere esattamente quali grandi banche dati o quali banche di sicurezza e di giustizia siano utilizzate nel nostro territorio.

Aggiungo che, al di là dei suddetti provvedimenti che dovranno indicare le banche dati in materia di sicurezza e di giustizia, ci sono anche altre banche dati strategiche che richiedono una particolare attenzione. Abbiamo già segnalato l'Anagrafe tributaria, ma pensiamo anche alle banche dati che si occupano di traffico telefonico. Anche in questo caso sarebbe opportuno che il Parlamento ci aiutasse a mettere a fuoco modalità idonee ad individuare queste grandi banche dati.

Potrebbe poi essere anche opportuno interrogarsi se arricchire e snellire, anche mediante previsioni espresse nel nostro codice, le funzioni del personale di polizia rispetto all'accertamento di violazioni della normativa *privacy*, in particolare per quelle che prevedono sanzioni amministrative, potenziando le ipotesi di contestazione diretta e di segnalazione all'Autorità anche ai fini dell'eventuale adozione di ulteriori provvedimenti.

Da ultimo riteniamo importante, anche sulla scia di una normativa già prevista nell'ordinamento italiano, la configurazione di una nuova ipotesi di reato da applicare almeno ai vertici aziendali che non abbiano vigilato adeguatamente sull'adozione delle misure di sicurezza da parte dei soggetti delegati all'interno delle aziende, delle società o delle istituzioni che utilizzano le grandi banche dati, o che per obbligo di legge debbono tenere archivi di dati relativi a cittadini di particolare pericolosità. Tale nuova ipotesi di reato consentirebbe di configurare una responsabilità penale specifica per mancata vigilanza da parte dei vertici aziendali.

Mi è sembrato doveroso svolgere tali considerazioni. Chiedo scusa per essermi dilungato, però ho ritenuto importante fornire una risposta specifica a ciascuna domanda posta. Soprattutto mi è sembrato doveroso cogliere l'occasione che ci avete fornito per esporvi una serie di indicazioni, richieste ed osservazioni circa le innovazioni che riteniamo necessarie per adempiere meglio ad un compito che – come ho cercato di evidenziare – considero sempre più importante e strategico. Mi permetto di aggiungere, senza eccessiva enfasi, ma credendoci profondamente, che tale

compito appare importante anche per assicurare il mantenimento delle condizioni di libertà e di democrazia nell'ordinamento italiano.

Ovviamente restiamo a completa disposizione per ogni ulteriore chiarimento o approfondimento che la Commissione ritenesse necessario.

PRESIDENTE. Presidente Pizzetti, la ringrazio a nome della Commissione per avere fornito risposte così puntuali alle questioni sollevate dai colleghi senatori.

Naturalmente non consideriamo completato qui il nostro rapporto perché alcune questioni sono tuttora aperte; nelle prossime settimane avremo sicuramente altre occasioni di incontro. Abbiamo preso atto dei suggerimenti che lei ha inteso fornire alla Commissione circa le modalità con cui può ulteriormente articolarsi il rapporto tra il Parlamento e l'Autorità.

Approfittando della disponibilità del presidente Pizzetti, invito i colleghi che intendano porre altre questioni o richieste di approfondimento a prendere la parola.

VILLONE (*Ulivo*). Signor Presidente, approfittando della disponibilità del presidente Pizzetti che, tra l'altro, è un caro amico e collega, vorrei sottoporgli qualche ulteriore considerazione.

Ho già posto attenzione alle nuove esigenze di protezione dei dati determinate dall'espansione delle tecnologie. In realtà, ritengo che ci troviamo di fronte a problemi antichi, cioè di ieri, ma anche a problemi di oggi e di domani. I problemi antichi sono quelli che forse più interessano, vale a dire quelli legati alle intercettazioni, alle violazioni delle banche dati. Sono antichi perché non incidono sulla filosofia, sull'impianto concettuale. Vi può essere una difficoltà derivante dal modificarsi delle condizioni della tecnologia applicata; può essere più o meno complicato difendere una banca dati, ma non c'è dubbio che essa vada difesa, così come non c'è dubbio che le intercettazioni illegali vadano bloccate.

Voglio sottoporre all'attenzione del presidente Pizzetti il fatto che sorgono alcune questioni che mettono in campo domande nuove, che ci costringono a guardare alle problematiche legate alla tutela della protezione dei dati personali in modo diverso. Ad esempio, va considerato che oggi abbiamo la possibilità di mettere insieme una sempre maggiore quantità di dati. Chiaramente, più i dati sono numerosi, meglio devono essere difesi. Questo è, appunto, il problema di ieri. Il problema di oggi e di domani è cosa ne facciamo di questa crescente mole di dati; peraltro, si tratta di una problematica che si sta già imponendo all'attenzione.

Supponiamo che sia possibile, ad esempio, disporre dei dati delle persone sfrattate per morosità e che ciò renda difficile la concessione di un mutuo da parte delle banche a questa categoria di cittadini. Come prima reazione affermeremmo che quel dato non dovrebbe essere conosciuto per evitare che la banca neghi a quelle persone il mutuo per l'acquisto di una casa. Tuttavia, la conoscibilità di quel dato non vi è dubbio che costituisca un elemento di correttezza del mercato: se impedissimo alla

banca di sapere che una tal persona è un cliente maggiormente a rischio peggioreremmo le condizioni nelle quali la banca svolge il proprio mestiere, e quindi le condizioni di tutti gli altri potenziali clienti.

Voglio anche portare un esempio relativo alla gestione dei servizi sanitari. Facciamo l'ipotesi che vi sia una banca dati nella quale sono inseriti tutti i dati relativi alle condizioni di salute dei cittadini: sembrerebbe una cosa mostruosa e la prima reazione, infatti, sarebbe quella di sopprimerla. Si tratterebbe, però, per altro verso di un potentissimo strumento per allocare correttamente le risorse pubbliche. Allora, sapendo che i sistemi sanitari stanno diventando sempre più costosi e sono ormai vicini alla soglia dell'insostenibilità, sarebbe giusto impedire la raccolta e la conservazione di informazioni tanto utili? Poniamo poi il caso che vi sia un'assicurazione integrativa privata in ambito sanitario: sarebbe giusto che il soggetto che eroga l'assicurazione conoscesse, dal punto di vista sanitario, tutto di tutti e potesse regolarsi quindi in ragione di questa conoscenza nella scelta di fare l'assicurazione? Si potrebbe affermare che nel primo caso, quello del servizio pubblico, il dato potrebbe essere utilizzabile e non nel secondo, quello dell'assicurazione integrativa volontaria e privata? Il livello di privatizzazione del servizio, infatti, potrebbe avere un impatto sulla risposta che può essere data.

Esaminiamo ora le ultime tecnologie, note come *push technology*. Ad esempio, se fossi avvocato, la mia segretaria potrebbe inviarmi un messaggio che automaticamente muterebbe la mia agenda senza che io sappia nulla, per cui sarei aggiornato in tempo reale; ciò, ovviamente, sarebbe molto utile. Questo specifico caso non rappresenta un problema dal punto di vista della *privacy*. Può accadere però che un imprenditore faccia lo stesso con il suo dipendente, oppure che quella tecnologia, come è possibile, venga utilizzata per controllare il dipendente, cioè per sapere, ad esempio, cosa ha fatto ad una determinata ora; sarebbe un po' come avere la telecamere in fabbrica.

Dunque, ci troviamo di fronte a questioni antiche, delle quali conosciamo già la risposta, anche se può essere complicato porla in essere, ma abbiamo di fronte anche questioni nuove rispetto alle quali non soltanto ci si chiede se c'è bisogno di più norme, ma anche se il sistema delle Autorità è quello giusto. I casi che ho indicato rientrano nella sfera di competenza di diverse Autorità, quella delle comunicazioni, quella della *privacy* e anche quella garante della concorrenza e del mercato. Sono aspetti che toccano quindi tre diverse Autorità, ognuna delle quali è portatrice di una missione specifica e particolare. La mia domanda è finalizzata a capire se questo è ancora il modello giusto; la questione non è avere più poteri, ma pensare a disposizioni diverse. Sono queste le considerazioni che rassego all'amico e collega Pizzetti.

*PIZZETTI*. Si tratta di argomenti affascinanti e il mio ringraziamento per aver posto tali questioni non è certamente formale. Da ultimo risponderò alla vera domanda, quella relativa a quale debba essere il modello dell'Autorità come tale, e quindi delle varie Autorità.

I punti toccati dal senatore Villone sono rilevanti e formano oggetto di una nostra continua riflessione. Su ciascuno di questi temi ho riflettuto moltissimo, anche a titolo individuale. Il primo problema da affrontare per noi va sotto il nome di centrale dei rischi. In una società come la nostra, che vive moltissimo di credito al consumo (la cosiddetta vendita a rate), c'è un'enorme attività di anticipazione da parte del venditore, che consegna il bene e sostanzialmente fa un prestito all'acquirente, che in seguito pagherà a rate. Quindi il venditore consegna il bene in tutto il suo valore, e poi sarà pagato secondo le modalità rateali convenute. Nella vecchia società esistevano garanzie reali a fronte del debito, come l'ipoteca o altre garanzie relative alle cambiali e ai titoli di credito. Ovviamente quelle garanzie, reali e non, che la società che ci ha preceduto aveva individuato, mal si adattano alle moderne necessità del mercato e della vendita rateale. Di qui la necessità di porsi un nuovo problema: come diminuire i rischi del venditore a fronte di una vendita nella quale il debitore può rivelarsi insolvente? Se guardassimo solo alla parte debole del rapporto potremmo essere indotti ad un giudizio non equilibrato. È chiaro, infatti, che se non si individuano adeguate forme di garanzia per il venditore, si otterrà semplicemente che la vendita rateale abbia un costo maggiore per tutti gli utenti: il venditore sarà portato a scaricare il rischio sull'interesse richiesto e la rata sarà più onerosa per tutti. Stesso discorso vale per qualsiasi soggetto che fornisca servizi attraverso modalità di pagamento differite (contratto di energia elettrica, telefonico, e così via). Siamo di fronte ad un problema delicatissimo.

Abbiamo una certa esperienza in materia di vendita al consumo – non a caso l'ho citata – e un codice deontologico, elaborato d'intesa con le centrali rischi operanti nel sistema italiano, che ha individuato una serie di principi in ordine alla conservazione nel tempo del dato del debitore insolvente, ma anche del debitore entrato nella cosiddetta lista nera perché ha omesso di pagare una rata, ma che successivamente ha onorato il debito contratto. Questo per evitare che un soggetto che magari nel mese di agosto è in vacanza e non ha pagato la rata del motorino del figlio finisca registrato in una centrale rischi che gli inibisce comunque l'acquisto rateale, anche se poi ha onorato il debito.

Quindi, in materia di vendita al consumo abbiamo un codice deontologico e una serie di criteri e alcuni punti di equilibrio ragionevole. Ci stiamo ponendo, attraverso un dibattito interno non facile, il problema se estendere o meno il sistema delle «centrali rischi» anche ai servizi telefonici. Le società telefoniche stanno chiedendo con una certa insistenza di poter essere ammesse al codice deontologico, o comunque di potersi avvalere delle centrali rischi, per poter verificare la solvibilità di colui che vuole sottoscrivere un contratto telefonico o acquistare un telefonino con relativo contratto. Si tratta di un argomento difficilissimo, che richiede un dibattito pubblico. Pertanto, alla domanda del senatore Villone, che chiede di sapere se è possibile che una Autorità in fondo indipendente, ma a contenuto fortemente tecnocratico, possa risolvere questi problemi nel chiuso della sua visione settoriale o debba invece riflettere e discu-

terne, rispondo che deve senz'altro discuterne approfonditamente con le istituzioni pubbliche.

Questo è il motivo per cui ritengo necessario un grande dibattito pubblico su tutti i temi di nostra competenza: conservazione delle banche dati, informazione ai cittadini dei rischi che i loro dati corrono, richiedendo quindi ai cittadini stessi, laddove sia possibile, un'autoprotezione. È necessario quindi un grande dibattito pubblico su come trovare punti di equilibrio quando sono in discussione valori fra di loro tutti meritevoli di attenzione ma contrastanti, come in questo caso. È facile parlare del punto di equilibrio tra libertà di informazione e riservatezza. Lo sappiamo tutti, è scritto all'articolo 21 della Costituzione. Ma per noi il problema dei punti di equilibrio da individuare si pone di continuo.

Per quanto concerne le banche sanitarie, il problema è ancora più complicato. Se il problema è l'uso dei dati sanitari ai fini dell'allocazione delle risorse, qualche risposta l'abbiamo già data. Con il Ministero dell'economia abbiamo trovato una soluzione di comune soddisfazione, consentendo l'invio dei dati relativi alla spesa sanitaria al suddetto Ministero in forma anonima. In tal modo il Ministero dell'economia può monitorare la spesa senza bisogno di sapere se quella determinata prestazione è stata fatta a favore di Tizio o di Caio, e quindi senza sapere chi dei due soffre della patologia che ha richiesto quell'incremento di spesa. Invece, se si individuano anomalie nei *trend* di spesa (per fare un esempio, a Torino un uomo di sessant'anni fa registrare un eccesso di spesa sanitaria in rapporto alla media dei suoi coetanei nella stessa città) si può chiedere alla ASL di svolgere un'indagine mirata. Quest'ultima, infatti, è legittimata a farlo in quanto è una struttura sanitaria, e quindi non viola la riservatezza del dato sanitario. Sarà quindi la ASL a dire al Ministero dell'economia se si è in presenza di un fenomeno anomalo che nasconde illeciti da parte del medico, del paziente o di altre strutture, o di un fenomeno che trova una spiegazione nel fatto che quella persona è affetta da una particolare patologia. In quel caso magari sarà opportuno verificare se in quella città vi sono condizioni che giustificano quella particolare patologia. Questo è anche il motivo per cui dobbiamo dare un parere sulle modalità di tenuta dei registri dei tumori nei luoghi di lavoro.

Le banche sanitarie comunque rappresentano il futuro, ma pongono già nel presente un'altra enorme problematica. La cartella sanitaria elettronica, che consente l'accesso a tutti i dati sanitari di un paziente ed ha la finalità di migliorare e rendere più efficiente la cura, presenta dei vantaggi ma può presentare anche dei problemi. Faccio l'esempio di un pronto soccorso che si vede portare un malato da un luogo diverso da quello di residenza. Se ha la possibilità immediata di accedere ai dati sanitari, può fornire una prestazione infinitamente più efficace proprio grazie alla conoscenza di questi dati. La pericolosità però è enorme. Esiste infatti il pericolo di accesso illecito, il rischio che i dati vengano conosciuti da chi non ha il diritto di conoscerli, sia esso l'assicuratore o il datore di lavoro, che potrebbe utilizzarli per fare scelte che tengano conto dello stato di salute del soggetto. Porto l'esempio di una persona che ha superato un concorso,



ma in virtù del tipo di malattie da cui è affetta viene scavalcata da un altro soggetto, meno capace ma più idoneo all'attività che il datore di lavoro privato intende far svolgere. In questo modo potrebbero crearsi gravissimi effetti discriminatori, attorno ai quali è necessario un grande dibattito pubblico.

Ma vi è di più. Mi riferisco alla pericolosità di gestire queste grandi banche dati se ciò non si accompagna a misure di sicurezza adeguate anche nell'immissione del dato. Faccio al proposito un esempio: se modifico il gruppo sanguigno del senatore Villone, con un'operazione di hackeraggio sul suo dato sanitario tenuto in una sede informatica, rischio di porre in essere il giallo perfetto: il pronto soccorso che cerca di salvarlo in realtà lo uccide perché fa una trasfusione con un gruppo sanguigno sbagliato.

Siamo quindi in presenza di questioni che richiedono un dibattito pubblico di tipo politico e valoriale, ma anche di problemi di carattere tecnico del tutto nuovi. È vero, senatore Villone, che ci stiamo riferendo ad una materia su cui da sempre siamo stati abituati a riflettere, ma che oggi assume una nuova dimensione proprio a fronte dei processi di smaterializzazione dei dati. Oggi è infatti possibile entrare in una banca dati senza farlo fisicamente, attraverso sistemi di hackeraggio o con altre modalità.

Quanto al settore assicurativo, è ovvia la nostra preoccupazione riguardo alle banche dati in materia sanitaria, posto che se un assicuratore viene a conoscenza dei dati sanitari di una persona, può acquisire notizie assolutamente in grado di orientarlo nella sua attività. Aggiungo che, nel caso in cui le compagnie assicuratrici potessero venire a conoscenza di tutti i dati sanitari dei loro clienti, verrebbe addirittura meno il concetto stesso di assicurazione. Tale concetto si fonda infatti sul principio del rischio e del calcolo delle probabilità, ed è evidente che se si fosse in grado di sapere di ogni soggetto che intende stipulare una polizza di assicurazione di carattere sanitario quali sono le aspettative di vita e le malattie, allora il rischio per la compagnia assicuratrice diventerebbe pari a zero, proprio perché non si sarebbe più di fronte ad un calcolo delle probabilità, ma alla conoscenza del rischio concreto rapportato a quel singolo assicurato; in tale ipotesi però avremmo palesemente cambiato le regole che presiedono alla stessa attività assicurativa.

Analogo discorso va fatto riguardo al rapporto tra imprenditore, datore di lavoro e lavoratore. In proposito abbiamo recentemente prodotto un corposo documento, che abbiamo chiamato «Linee guida» – peraltro è la prima volta che l'Autorità adotta il criterio di pubblicare delle linee guida sulla *Gazzetta Ufficiale* –, nelle quali abbiamo riassunto tutta una serie di principi, di norme e di interpretazioni riguardanti il suddetto rapporto e finalizzate ad evitare una utilizzazione illecita dei dati dei lavoratori da parte del datore di lavoro, in contrasto con la normativa in materia di *privacy*.

Al riguardo siamo però consapevoli del fatto che ancora oggi spesso si è prigionieri di una visione del mondo del lavoro organizzato secondo modalità in cui il datore di lavoro e il lavoratore sono percepiti come parti contrapposte, come degli antagonisti nell'ambito di una relazione in cui il

lavoratore è la parte debole e il datore di lavoro quella forte, il che non sempre corrisponde alla realtà, ed è per questo che diventa necessario inquadrare il problema in un altro panorama.

Da questo punto di vista, un esempio può essere quello della localizzazione del lavoratore, che di per sé certamente costituisce una forma di controllo a distanza del lavoratore, ma se quest'ultimo è l'autista di un portavalori o comunque di un furgone che trasporta merci preziose è evidente che il controllo a distanza diventa una misura di sicurezza a tutela dello stesso lavoratore. Ancora: la videocamera installata nella agenzia bancaria, finalizzata ad evitare le rapine, rappresenta certamente anche un modo per controllare il comportamento dei dipendenti, perché se essa è puntata sugli sportelli è evidente che riprenderà anche l'attività degli operatori. In questo caso si rientra nell'ambito di un'altra problematica che riguarda le modalità con cui questi dati sono raccolti, il diritto di accesso agli stessi e le finalità con cui essi possono essere utilizzati.

Sempre in tal senso credo sia interessante una decisione del Garante adottata nei mesi scorsi. È stata avanzata ed accolta dall'Autorità la richiesta di poter accoppiare, ai fini di una maggiore sicurezza delle agenzie bancarie, l'acquisizione dell'impronta biometrica del cliente, necessaria a consentirne l'ingresso nella banca, ai filmati delle videocamere; in questo caso è però evidente che, a fronte di una maggiore tutela, si accentui contemporaneamente anche la pericolosità del trattamento dei dati, posto che si viene a conoscenza anche delle fattezze della persona che ha lasciato l'impronta biometrica, che non servirà a identificare l'eventuale rapinatore, bensì il cliente, associando, appunto, impronta, viso e caratteristiche somatiche; e si tratta di dati che possono essere utilizzati per scopi e finalità lesivi del cliente stesso.

Ebbene, in questo caso il Garante ha suggerito di ricorrere ad un «vigilante dei dati», e ha stabilito che i dati relativi alle impronte digitali e quelli delle riprese video debbano essere contenuti in archivi separati e possano essere connessi fra di loro solo nell'eventualità che emergano determinate esigenze, e che in ogni caso ciò avvenga sotto il controllo di un soggetto terzo, individuato dalla banca, ma estraneo al suo apparato, ciò proprio al fine di ampliare i livelli di sicurezza.

Ho citato questo esempio proprio per evidenziare la complessità della nostra attività. Guardando anche alla esperienza che ciascuno di noi ha maturato nella propria vita professionale, quanto detto sta a dimostrare che non si può rispondere in modo univoco alla domanda sull'opportunità che certe problematiche continuino ad essere di competenza dell'Autorità, oppure se sia più corretto che al riguardo abbia luogo un dibattito pubblico.

Personalmente ritengo valide entrambe le ipotesi. Infatti, se da una parte siamo in presenza di una materia tecnica e complessa di problematiche che solo un corpo specializzato come quello dell'ufficio di un'Autorità e di un organo collegiale che ha ricevuto la fiducia del Parlamento è in grado di valutare in tutte le sue sfaccettature e implicazioni, dall'altra sono assolutamente convinto che non sia possibile e che sarebbe contro

ogni ragionevolezza, prima che contro ogni principio democratico, immaginare che solo un tale soggetto possa essere il titolare del compito delicatissimo di trovare il giusto punto di equilibrio tra esigenze contrapposte. Questa è la ragione per cui ritengo fondamentale il rapporto con il Parlamento e, conseguentemente, essenziale questo tipo di dibattito e dialogo, ma è anche il motivo per cui, quando è possibile, partecipiamo a trasmissioni televisive e a tutte le occasioni in cui sia possibile stimolare il dibattito pubblico su questi temi.

Ad esempio, la nota vicenda del servizio degli inviati della trasmissione «Le Iene» è stata preziosa in questo senso, proprio perché ha fatto capire all'opinione pubblica che basta un tampone per registrare dati che riguardano la salute di una persona, fino addirittura a raccogliere delicatissime informazioni sull'utilizzo o meno di sostanze stupefacenti. Si tratta di forme di indagine che potrebbero magari in futuro essere volte ad accertare l'uso di determinati farmaci tipici di una certa malattia, con il rischio di ricadute terrificanti per le persone che siano vittime di questo tipo di attività.

Quindi siamo favorevoli ad un modello dell'Autorità all'interno di un contesto in cui l'Autorità stessa non si senta chiusa in una torre d'avorio, né abbia la presunzione di essere sovranamente il *dominus* del problema politico costituito dall'individuazione del punto di equilibrio fra i diversi valori; questo, ovviamente, vale anche per le Autorità europee, quindi per la *working party* che troppe volte opera come se fosse chiuso in una sfera di cristallo, in una sorta di boccia dei pesci rossi, come se si trattasse di un mondo a sé stante. Ovviamente la difficoltà è nel trovare il punto di equilibrio cui facevo riferimento.

Quanto poi al tema della ripartizione delle competenze tra le varie Autorità, credo che per affrontarlo sarebbe necessario ricominciare il dibattito; mi limiterò pertanto a sottolineare che effettivamente ci differenziamo dalle altre perché siamo una Autorità a tutela dei diritti, tant'è che siamo l'unica i cui i provvedimenti sono ricorribili davanti al giudice ordinario e non davanti a quello amministrativo. Un'altro aspetto che ci caratterizza e distingue dalle altre Autorità è l'enorme ampiezza dei settori di nostra competenza, essendo il Garante preposto a tutelare i dati, ovvero l'elemento che ormai costituisce il sangue che scorre nelle vene di tutta la società; ne consegue che, per definizione, la nostra Autorità è ben più plurisetoriale e trasversale delle consorelle.

PRESIDENTE. Ringrazio il professor Pizzetti ed i suoi collaboratori per il prezioso contributo offerto ai lavori della nostra Commissione.

Dichiaro conclusa l'audizione e rinvio il seguito dell'indagine conoscitiva ad altra seduta.

*I lavori terminano alle ore 15,45.*

