

**COMMISSIONE XIV
POLITICHE DELL'UNIONE EUROPEA**

RESOCONTO STENOGRAFICO

AUDIZIONE

7.

SEDUTA DI MERCOLEDÌ 28 NOVEMBRE 2007

PRESIDENZA DEL PRESIDENTE **FRANCA BIMBI**

INDICE

	PAG.		PAG.
Sulla pubblicità dei lavori:		<i>(ai sensi dell'articolo 143, comma 2, del Regolamento):</i>	
Bimbi Franca, <i>Presidente</i>	3	Bimbi Franca, <i>Presidente</i>	3, 10, 11, 12, 14 15, 17, 19, 22, 24
Audizione del presidente dell'Autorità garante per la protezione dei dati personali, professor Francesco Pizzetti, nell'ambito dell'esame dei disegni di legge C. 2630 e C. 2711 (ratifica di accordi sul sistema di navigazione satellitare Galileo), sugli aspetti concernenti la tutela dei dati personali nel contesto normativo comunitario		Cassola Arnold (Verdi)	10, 22
		De Biasi Emilia Grazia (PD-U)	15
		Frigato Gabriele (PD-U)	17
		Picano Angelo (Pop-Udeur)	17
		Pini Gianluca (LNP)	11, 14, 15
		Pizzetti Francesco, <i>Presidente dell'Autorità garante per la protezione dei dati personali</i>	3, 12, 14, 15, 20, 22

N. B. Sigle dei gruppi parlamentari: Partito Democratico-L'Ulivo: PD-U; Forza Italia: FI; Alleanza Nazionale: AN; Rifondazione Comunista-Sinistra Europea: RC-SE; UDC (Unione dei Democratici Cristiani e dei Democratici di Centro): UDC; Lega Nord Padania: LNP; Sinistra Democratica. Per il Socialismo europeo: SDpSE; Italia dei Valori: IdV; La Rosa nel Pugno: RosanelPugno; Comunisti Italiani: Com.It; Verdi: Verdi; Popolari-Udeur: Pop-Udeur; DCA-Democrazia Cristiana per le Autonomie-Partito Socialista-Nuovo PSI: DCA-NPSI; Misto: Misto; Misto-Minoranze linguistiche: Misto-Min.ling.; Misto-Movimento per l'Autonomia: Misto-MpA; Misto-Repubblicani, Liberali, Riformatori: Misto-RLR; Misto-La Destra: Misto-Destra; Misto-Socialisti per la Costituente: Misto-SocpC.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE
FRANCA BIMBI

La seduta comincia alle 10,05.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso e la trasmissione televisiva sul canale satellitare della Camera dei deputati.

Audizione del presidente dell'Autorità garante per la protezione dei dati personali, professor Francesco Pizzetti, nell'ambito dell'esame dei disegni di legge C. 2630 e C. 2711 (ratifica di accordi sul sistema di navigazione satellitare Galileo), sugli aspetti concernenti la tutela dei dati personali nel contesto normativo comunitario.

PRESIDENTE. L'ordine del giorno reca, ai sensi dell'articolo 143, comma 2, del Regolamento, l'audizione del presidente dell'Autorità garante per la protezione dei dati personali, professor Francesco Pizzetti, nell'ambito dell'esame dei disegni di legge C. 2630 e C. 2711 (ratifica di accordi sul sistema di navigazione satellitare Galileo), sugli aspetti concernenti la tutela dei dati personali nel contesto normativo comunitario.

In particolare, il presidente Pizzetti è stato invitato a intervenire affinché la Commissione acquisisca gli strumenti necessari per approfondire i temi legati alla tutela dei dati personali, nel contesto normativo italiano e comunitario.

È chiaro che non abbiamo le competenze per entrare nei meriti della questione, mentre le abbiamo per capire come, in questo caso specifico, la materia della tutela dei dati personali si articola tra la legislazione italiana e le normative comunitarie. In questo ambito, peraltro, occorre considerare che il sistema satellitare si interfaccia anche con contesti di legislazioni non comunitarie e internazionali.

Tuttavia, ho circoscritto l'ambito del nostro interesse perché tale tematica non è affatto secondaria e rientra nel discorso dell'integrazione europea, sia dal punto di vista delle tecnologie che da quello dei diritti.

Nel ringraziare il professor Pizzetti per aver accolto il nostro invito, gli cedo la parola.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Ringrazio il presidente e la Commissione per l'opportunità che viene data a me, e soprattutto all'Autorità, di esprimere le nostre valutazioni sulla tematica in esame.

Dico subito che, rispetto allo specifico argomento di cui la Commissione si sta occupando, ossia i disegni di legge di ratifica di tre accordi tra la Comunità europea, gli Stati membri, la Cina, gli Stati Uniti d'America e Israele, a noi sembra di non avere specifiche obiezioni od osservazioni da fare.

Si tratta di accordi che, sostanzialmente, hanno un contenuto tecnico. In due casi, essi tendono a favorire l'interoperabilità tra il sistema Galileo, ancora in corso di realizzazione, e i sistemi già operanti, in particolare negli Stati Uniti e in Cina, o a consentire, anche allo Stato di Israele, di partecipare alla realizza-

zione del sistema Galileo o di servirsi in futuro di esso.

In ogni caso, tali accordi di per sé non coinvolgono il trattamento di dati personali, riguardando piuttosto la interoperabilità tra i sistemi.

Credo che, da questo punto di vista, gli accordi possano essere considerati favorevolmente sotto diversi aspetti, sia per le opportunità che danno agli utenti dell'uno e dell'altro sistema, grazie appunto all'interoperabilità, sia per la creazione di occasioni e prospettive di sviluppo tecnologico e di utilizzo per le società, le imprese e le strutture dell'Unione europea che sono impegnate nella realizzazione del sistema Galileo.

Si potrebbe immaginare che, laddove l'attività e l'operatività di questi sistemi implichi un trattamento di dati personali, vi sia anche uno specifico interesse a richiamare la competenza dell'Autorità garante italiana per tutelare i dati dei cittadini trattati nell'ambito del territorio italiano. Tuttavia, già il codice in materia di protezione dei dati personali (il decreto legislativo n. 196 del 2003) contiene una serie di norme anticipatrici in questo settore, anche in coerenza con la direttiva europea n. 2002/58/CE, e copre queste ipotesi.

Da questo punto di vista, dunque, ci sembra di non avere rilevanti osservazioni da fare, salvo riservarci di fornire tutte le ulteriori delucidazioni che si dovessero rendere necessarie o venissero richieste.

Invece, ci pare interessante cogliere l'occasione per comunicare le nostre conoscenze in ordine al sistema Galileo, ma soprattutto in merito al processo in atto nell'ambito dell'Unione europea — ma possiamo dire a livello mondiale —, per quanto riguarda l'uso di questi nuovi sistemi di navigazione satellitare.

Come sapete, il programma Galileo è una scelta che l'Unione europea ha compiuto e che è destinata a inserirsi nell'ambito di una politica europea più ampia, che ha già portato, con il regolamento n. 1321 del 2004, all'istituzione di un'Autorità di vigilanza europea sul sistema

globale di radio navigazione satellitare GNSS (*Global navigation satellite system*).

Tale sistema, creato dall'Unione europea, raggiungerà la sua piena funzionalità quando sarà perfettamente operativo anche il sistema Galileo, che ne enfatizzerà e ne consentirà il miglior funzionamento.

Il sistema Galileo, in sé e per sé, si evidenzia rispetto agli altri, in particolare al GPS degli Stati Uniti, oggi sicuramente più noto, per essere stato concepito fin dall'inizio come un sistema di trasmissione di segnali, ai fini della radio navigazione satellitare, sotto organizzazione totalmente civile. Il sistema GPS americano, invece, è, e rimane, sotto organizzazione prevalentemente militare.

Tale dato di fatto comporta una serie di conseguenze già nella realtà attuale. Naturalmente, essendo sotto il controllo della Difesa americana, il GPS ha una serie di modalità e potenzialità operative che possono essere condizionate direttamente dalle esigenze della Difesa stessa. Penso, ad esempio, alla possibilità di interrompere o rendere più difficile la ricezione del segnale, per esigenze di difesa interne ed esterne degli Stati Uniti.

Il sistema Galileo, invece, è stato concepito fin dall'inizio come un sistema sotto controllo e per finalità essenzialmente civili. Ovviamente, ciò non toglie che anche questo sistema, come tutti quelli funzionali al trattamento dati, possa essere poi oggetto di specifiche prescrizioni o utilizzazioni anche per ragioni di sicurezza pubblica o di difesa. La sua concezione, tuttavia, è diversa. Viene concepito come un servizio civile, sotto organizzazione civile, destinato ad entrare nel sistema dell'agenzia europea di cui abbiamo parlato poc'anzi, ma che è improntato, prima di tutto, a fornire essenzialmente servizi civili.

Al contrario, come ho detto, il GPS americano nasce, e resta caratterizzato, dalla essenziale finalità strategica a fini di difesa, anche se è utilizzabile per scopi civili.

Galileo è un sistema di satelliti che trasmettono a terra dei segnali finalizzati a consentire al soggetto che li riceve di

stabilire la propria posizione e di rilevare l'ora esatta con estrema accuratezza. Pertanto, in sé e per sé, il sistema Galileo, come sistema satellitare, non implica un trattamento di dati, non registra e non trasmette dati, limitandosi a funzionare come una sorta di radiofaro.

Il sistema Galileo è concepito, in particolare, per fornire cinque diverse tipologie di servizi.

Alcuni servizi sono definiti di base, sono aperti e destinati a servizi di interesse generale che consentono la localizzazione, attraverso il sistema che ho cercato di descrivere, del soggetto che ha deciso di avvalersene dotandosi delle necessarie apparecchiature di ricezione.

Vi sono poi i servizi commerciali. Già in quest'ambito possiamo immaginare le possibili diverse utilizzazioni: ad esempio — per capire meglio il contesto del quale parliamo — si possono prospettare, al titolare dell'apparecchio ricevitore, offerte commerciali specifiche a seconda della zona nella quale lo stesso si trova.

Questo è ciò che normalmente vediamo nei film che crediamo di fantascienza ma che, invece, anticipano o semplicemente descrivono una realtà già in corso.

Insomma, sto parlando di un sistema grazie al quale, se viaggio con il mio telefonino a bordo di un'automobile in una determinata zona di una certa nazione, ho la possibilità di ricevere le pubblicità dei ristoranti o dei grandi magazzini collocati in quell'area. Infatti, localizzando la mia posizione, il sistema di servizio commerciale può inviarmi delle offerte connesse specificamente alla zona in cui mi trovo. Ho citato questo caso solo perché, avendolo visto nei film, è uno degli esempi più facilmente comprensibili da ciascuno di noi, indipendentemente dalle singole e specifiche competenze professionali.

Il terzo tipo di servizio è quello chiamato « *safety of life* ». Ovviamente, questa è una definizione generica che comprende una grande quantità di utilizzazioni ai fini salvavita, dalla localizzazione del disperso sotto una valanga, fino ad altre ipotesi che possiamo immaginare, e che contiene an-

che un servizio più specifico quello di ricerca e salvataggio delle persone in pericolo. Per intenderci, mi riferisco a circostanze come quella che si è verificata nel caso del famoso navigatore che, disperso nel Pacifico, è stato localizzato grazie a questo tipo di sistema.

Infine, vi sono i servizi dedicati all'utenza cosiddetta « istituzionale », che è già previsto avvengano attraverso forme di trasmissione e ricezione di un segnale criptato e maggiormente tutelato da radiodisturbi o interferenze. Questo tipo di servizio è concepito per finalità di protezione civile, sicurezza nazionale, tutela dell'ordine pubblico e rispetto della legge.

Parliamo, dunque, di un sistema di ripetitori orbitanti che, in quanto tali, sono finalizzati a consentire la localizzazione dell'apparecchio che riceve il segnale dai satelliti Galileo, cui si affiancano impianti di trasmissione a terra e sistemi di elaborazione che consentono la fornitura di servizi a valore aggiunto, che presuppongono tuttavia l'esistenza di un « canale di ritorno » con cui l'utente può comunicare a dei « centri servizi », automaticamente o, di volta in volta, di propria iniziativa, la posizione acquisita tramite il sistema satellitare.

Tali ripetitori, tuttavia, sono concepiti anche per poter essere utilizzati secondo cinque diverse categorie e tipologie di servizi definiti, tramite queste etichette generiche, come servizi aperti per i diversi usi civili, servizi commerciali, servizi salvavita, servizi di ricerca e salvataggio e servizi di utenza istituzionale.

Ai fini della protezione dati, i problemi possono nascere quando questi servizi vengono utilizzati per una eventuale registrazione dei dati raccolti nell'ambito della fornitura di quei servizi aggiuntivi. Intendo dire che la eventuale registrazione e archiviazione dei dati non solo per la finalità specifica di fornire il servizio di volta in volta previsto, ma anche solo per mantenere memoria del segnale o delle informazioni ricevute, può incidere pesantemente sulla tracciabilità e conoscibilità dei movimenti delle persone a cui sono riconducibili le informazioni medesime.

Viceversa, se questo non avviene, la pericolosità ai fini del trattamento dati di questi servizi diminuisce in modo significativo.

È anche evidente che, a seconda del tipo di servizio del quale parliamo, nascono problemi legati alla consapevolezza da parte del possessore e, dunque, relativi anche al consenso che può essere richiesto al soggetto per consentirgli di avvalersi di tale servizio; nascono problemi rispetto alla possibilità che gli viene data, o non viene sufficientemente garantita, di rinunciare in qualunque momento al servizio previsto.

Detto in altri termini, diventa molto importante sapere che esiste un servizio salvavita, o di ricerca delle persone, un servizio a fini commerciali o professionali o, come abbiamo detto, un servizio aperto.

Un servizio di questo ultimo tipo può interessare, ad esempio, un trasportatore che desidera che i *container*, eventualmente trasportati via mare, siano localizzabili in qualunque momento, nell'ambito dell'intero tragitto che va dal porto di partenza a quello di destinazione della merce. Ovviamente, per poterlo fare, occorre sapere che esiste tale servizio e bisogna essere in grado di dare il consenso al trattamento dei dati personali, così come di ritirare detto consenso in qualunque momento.

L'esempio che ho citato però coinvolge anche l'intero equipaggio della nave. Infatti, localizzando un *container* su di una nave, si localizza inevitabilmente anche l'equipaggio della stessa che, pertanto, deve essere posto nella condizione di rinunciare, nell'ambito dello svolgimento della propria attività lavorativa, alla possibilità di essere localizzato.

Si tratta di problemi complessi che le Autorità garanti di protezione dei dati hanno comunque più volte affrontato.

Lo stesso discorso vale per l'utilizzazione individuale, nel caso in cui una persona decida che è suo interesse essere localizzata, o scelga di avvalersi del navigatore satellitare sulla propria automobile. Tuttavia, in un determinato momento, per una qualunque ragione complessa o deli-

cata, di carattere sentimentale o di altro genere, può decidere di rinunciare al servizio offerto, per essere sicuro che la propria vettura non sia più localizzabile. Intende cioè sottrarsi consapevolmente alla possibilità di essere localizzato, rinunciando ai benefici che una tale localizzazione può comportare e decidendo, consapevolmente, di correre, invece, determinati rischi.

Tutta questa tematica — che sto descrivendo in termini sintetici e in parte approssimativi — è stata, è, e sarà oggetto di approfondimenti costanti da parte non solo dei soggetti chiamati a organizzare e gestire questi servizi, ma anche delle Autorità garanti.

Devo dire che l'Unione europea è particolarmente attenta e sensibile a queste problematiche. Già la direttiva n. 58 del 2002, in materia di telecomunicazioni, conteneva norme importanti. Infatti, nell'ambito dei dati relativi ai sistemi di telecomunicazione, essa ha distinto specificamente quelli necessari a consentire l'utilizzo di un servizio specifico — mi riferisco, per intenderci, a quello per telefonare o inviare *e-mail* — dai dati che, invece, sono utilizzabili per fornire i cosiddetti servizi a valore aggiunto, ossia servizi diversi che non hanno nulla a che fare con le comunicazioni tradizionalmente intese.

Quindi, il segnale che può essere utilizzato dal mio telefonino per mettermi in contatto con un'altra persona e parlarle entra all'interno di un certo sistema di protezione dati. Il segnale inviato dal mio telefonino che, invece, può essere utilizzato per consentirmi, avendo scelto che questo avvenga, di essere localizzato in qualunque momento (quindi, se mi perdo, mi permette di essere facilmente rintracciabile da un servizio salvavita) è da trattare secondo modalità e con tipi di precauzione differenti.

Infatti, mentre nel primo caso parliamo di un dato finalizzato specificamente al sistema di comunicazione, nel secondo ci riferiamo a un dato che viene utilizzato per scopi diversi dalla comunicazione intesa in senso proprio. Parlo, dunque, di un

servizio a valore aggiunto, che può essere fornito avvalendosi di un segnale che, pur percorrendo il sistema delle telecomunicazioni, ha finalità diverse.

Questa distinzione è stata molto importante, perché ha consentito di sottoporre a misure specifiche e diverse il trattamento dell'uno e dell'altro tipo di dato.

Anche per il gestore telefonico è consentito trattenere e archiviare i dati relativi ai servizi di telecomunicazione tradizionalmente intesi, secondo certe modalità. I dati che invece vengono utilizzati per offrire i cosiddetti servizi a valore aggiunto devono essere trattati secondo altre modalità, differentemente individuate. Peraltro, è evidente che i due tipi di dati avranno anche un diverso valore per quanto riguarda le indagini giudiziarie, il loro utilizzo ai fini di giustizia o di archiviazione presso le autorità giudiziaria o di pubblica sicurezza.

Inoltre, in modo molto significativo, la distinzione che è stata effettuata è importante anche nei confronti dell'utente.

In linea di massima, per dare degli spunti di riferimento, si può precisare che per i servizi a valore aggiunto deve essere sempre fornita un'informativa chiara che metta l'utente nelle condizioni di capire esattamente, nel momento in cui sottoscrive un servizio, rispetto a quale trattamento dati esprime il proprio consenso.

In secondo luogo, deve essere sempre possibile revocare il consenso informato e, dunque, rinunciare all'utilizzazione di questo servizio, in un qualunque momento si cambi - per usare un termine molto generico - opinione.

Il terzo problema molto delicato è legato all'archiviazione dei dati utilizzati per fornire i servizi a valore aggiunto.

Mentre per i dati connessi al traffico telefonico il regime di conservazione tiene presente la specificità del servizio offerto, per i servizi a valore aggiunto, si stabilisce che il gestore non deve registrare i dati. Colui che fornisce il servizio li potrà registrare solo per la finalità specifica della fornitura del servizio e, eventualmente, per fini di fatturazione.

Per tutto quel che riguarda le fasi successive, invece, la normativa non coincide con quella del traffico telefonico di telecomunicazione in senso proprio.

Infine, vorrei affrontare due problemi specifici. Innanzitutto, si pone una questione molto delicata e complessa per quanto riguarda i lavoratori. Del resto, capite che - per usare termini non tecnici - l'interesse dell'impresa può essere ben diverso da quello dei lavoratori.

L'impresa può avere interesse a localizzare in qualunque momento le merci oggetto dell'attività economica, può voler sapere con quale velocità avviene la consegna dei prodotti, quale percorso viene seguito, o secondo quali modalità il trasportatore opera nella sua attività lavorativa. Per contro, questo può significare aprire la via a un controllo a distanza sul lavoratore.

Non è facile trovare una soluzione. I Garanti europei se ne sono occupati molto e hanno scelto la via più garantista, prevedendo cioè la possibilità che in qualunque momento il lavoratore, o chiunque stia utilizzando il servizio, possa disattivare il sistema che ne consente la localizzazione.

D'altra parte, si pongono anche problemi di sicurezza. Da questo punto di vista, la situazione è simile a quella che si determina quando si dà la possibilità ai commessi di un negozio di scrivere in un cartello che non ci sono soldi in cassa in quanto il denaro viene immediatamente messo in cassaforte.

Agendo in questo modo, si risolve un problema di sicurezza, ma si può anche mettere a rischio l'incolumità del personale.

Infatti, da una parte, il commesso è inerme innanzi un rapinatore, non potendo aprire la cassaforte; ma, dall'altra parte, si può mettere maggiormente a rischio la vita del commesso medesimo, perché il rapinatore potrebbe essere colto da un raptus di violenza aggiuntivo proprio perché il commesso è nella impossibilità di consegnarli il denaro richiesto.

Nel caso di un lavoratore che stia trasportando merce di particolare valore,

il fatto che il mezzo di trasporto sia costantemente localizzato rappresenta una misura di sicurezza. Tuttavia, se si consente — come i Garanti europei chiedono che si faccia — di disattivare il servizio in qualunque momento, per sottrarsi a un controllo oppressivo del datore di lavoro, questo può anche diventare un elemento di insicurezza. Infatti, una volta salito a bordo del mezzo di trasporto, sotto minaccia della pistola, il rapinatore può intimare di disattivare il localizzatore, rendendo così il lavoratore totalmente preda della sua violenza.

Quindi, quando operiamo in questi settori, ci troviamo sempre in una posizione scomoda e delicata.

Voglio ricordare l'iniziativa dei Garanti europei che si sono occupati anche dei localizzatori salvavita. È stata avanzata a livello europeo una proposta molto costosa, che probabilmente non troverà attuazione in tempi brevi, chiamata «*E-call*». Si tratta di un progetto proposto con lo scopo di ridurre il costo, in vite umane e in termini economici, degli incidenti stradali che avvengono sulle strade europee, stimato in cifre molto alte (circa 40 mila morti l'anno).

La Commissione europea ha prospettato la possibilità di dotare obbligatoriamente le automobili di nuova fabbricazione di un sistema di localizzazione, a finalità unicamente salvavita. In caso di *crash*, quando si determini un impatto violento al di sopra di una certa velocità (diciamo 40 chilometri all'ora), attraverso una localizzazione in automatico, tale sistema contatterebbe i servizi di soccorso, vigili del fuoco, meccanici, o sanitari, accelerandone l'arrivo sul luogo ove si è verificato l'incidente. Tale sistema dovrebbe essere in grado di abbassare i costi in vite umane e in termini economici degli incidenti sulle strade europee.

I Garanti europei si sono profondamente interrogati su questo nuovo sistema, perché, come capite, anche da questo punto di vista il sistema presenta vantaggi e svantaggi. Ad esempio, ci si può trovare ad essere improvvisamente destinatari dell'arrivo di mezzi di soccorso, semplice-

mente perché si è compiuta una manovra azzardata e si è andati a sbattere contro un platano. Dunque, anche nel caso in cui non si sia verificato un incidente mortale, potrebbe scattare il sistema di *E-call*, rendendo il soggetto totalmente privo di ogni riservatezza, semplicemente perché si è attivato il segnale salvavita.

Per contro, se questo segnale deve essere — come i Garanti europei richiedono — sempre disattivabile dall'automobilista, proprio al fine di garantire la riservatezza necessaria, può capitare di disattivarlo per le motivazioni più diverse e poi ritrovarsi impossibilitati ad avere il soccorso salvavita.

Quindi, sia che si parli di controllo sui lavoratori che, più in generale, delle possibilità di disattivazione dei vari sistemi di localizzazione, si devono sempre avere presenti i pro e i contro dati dalle diverse situazioni.

Ovviamente, la linea di azione dei Garanti europei è sempre orientata alla massima tutela della riservatezza e, quindi, alla possibilità di disattivare comunque e in ogni momento i sistemi che consentono la localizzazione degli individui.

Un ulteriore problema, anche questo delicato e complesso, è legato ai minori. In particolare, si tratta di stabilire a quale età dobbiamo riconoscere al minore la maturità sufficiente per essere libero di decidere se attivare o disattivare i sistemi di localizzazione.

Lo ripeto, questo ragionamento include sia i sistemi satellitari, sia quelli che non lo sono e che sono molto più semplici. Penso, ad esempio, all'*RFID (Radio frequency identification)*, che può essere indossato come un braccialetto da un bambino e che ne può consentire la localizzazione immediata nel caso in cui si perdesse, ad esempio in spiaggia, evitando così alla madre ricerche difficili.

Ebbene, dunque, a quale età è giusto dare la possibilità di attivare o disattivare i sistemi di localizzazione? Anche a questo proposito, i Garanti europei si sono interrogati a fondo. Si tratta di un problema molto delicato. Non ci si può limitare semplicemente a consentire ai minori di

disattivare i sistemi di localizzazione, impedendo così alle madri di ritrovarli facilmente e in qualunque momento.

Al tempo stesso, dobbiamo capire le ragioni di ragazzi di 16 o 17 anni, e forse anche dei quindicenni, che possono avvertire l'esigenza di non essere sempre sotto il controllo permanente dei propri genitori.

Vengo ora alla conclusione di questa introduzione, che ho voluto deliberatamente rendere discorsiva. Avrei potuto esporvi aspetti di carattere maggiormente tecnico, ma mi pare che in questa occasione sia importante capire quali sono le questioni in ballo.

Infine, occorre tenere presente che anche il concetto di sicurezza interna ed esterna può dilatarsi molto.

Nel caso dell'*E-call* e dell'*anticrash*, ad esempio, si può decidere di dare una prevalenza forte all'interesse pubblico a salvare anche chi non volesse essere salvato e, dunque, all'interesse ad impedire, a chi volesse farlo, di liberarsi del controllo, perché si considera prioritario l'interesse non del singolo ma della collettività.

Anche in questo caso, si potrebbero avere delle buone ragioni per decidere di seguire tale direzione. Infatti, si può anche ritenere che lo sciatore, o l'alpinista, che azzarda una scalata in condizioni inadeguate di sicurezza, e che intende sottrarsi alla localizzazione, ci guadagna in libertà, ma indubbiamente potrebbe mettere a rischio la vita dei soccorritori.

Del resto, un conto è portare avanti un'attività di soccorso mirata con un sistema che consente una localizzazione sicura e precisa del soggetto disperso; altra cosa è, invece, prestare soccorso senza questo ausilio, nel caso in cui la persona abbia volutamente disattivato il servizio, sottraendosi di proposito alla possibilità di ricorrere a questo mezzo salvavita.

Si può ritenere, ad esempio, che la localizzazione di persone, o di barche, in zone a rischio di una certa parte dell'oceano non possa essere disattivata, ai fini di usi di sicurezza salvavita. Infatti, se arriva un ciclone, si ha interesse a localizzare immediatamente la nave, per sal-

vare l'equipaggio, mettendo molto meno a rischio le strutture di sicurezza finalizzate al salvataggio di quanto invece sarebbero se si fosse liberamente scelto di disattivare il sistema di localizzazione.

Quindi, quando parliamo di usi civili obbligatori, di usi legati al sistema istituzionale, o di usi non civili di sicurezza interna ed esterna, o attività di giustizia, entriamo in uno scenario del tutto nuovo, in cui l'interesse pubblico assume una rilevanza particolare ed è costantemente in bilico con il diritto del soggetto a sottrarsi al controllo.

Per riassumere, abbiamo di fronte una serie di problemi complessi: la possibilità di sottrarsi al controllo, come elemento di libertà, e la possibilità, invece, di essere sottoposti a controllo anche senza consenso.

Si pongono, dunque, diversi argomenti alla nostra riflessione. Uno di questi riguarda la ricerca dell'equilibrio tra i diversi valori in gioco e le modalità con le quali garantire che la persona interessata sia davvero nelle condizioni di essere consapevole delle proprie scelte.

Intendo dire che occorre chiarire in che modo gli utenti devono essere informati e quale tipo di consenso deve essere richiesto loro. Un conto è chiedere un consenso formale, altro conto è fornire spiegazioni sufficienti affinché le persone siano consapevoli di quello che fanno, ivi compresa la necessità di renderli capaci di scegliere tra i diversi valori in gioco.

Del resto, se ci si limita a chiedere ad una persona se intende poter disattivare il localizzatore in qualunque momento, questa potrebbe anche rispondere affermativamente. Tuttavia, credo che sia necessario e responsabile avvertire la stessa persona che, una volta disattivato il servizio, a fronte di una maggiore libertà, si avranno anche una serie di conseguenze potenzialmente negative. Dunque, soltanto dopo aver messo al corrente l'interessato di tutti gli aspetti utili e dei possibili svantaggi, questi potrà decidere in maniera consapevole se attivare o disattivare il localizzatore.

È necessario, quindi, svolgere un enorme lavoro di informazione non solo puramente giuridica e tecnica, ma anche, e soprattutto, come diffusione di una maggiore consapevolezza.

Ritengo che in questa materia si debba sostituire sempre più la richiesta di un consenso con il concetto di una effettiva consapevolezza. Il termine « consenso » è molto formale, il termine « consapevolezza » è invece sostanziale e richiede, da parte di chi dà l'informazione, un dovere di spiegazione ampio e molteplice.

Oltre a ciò, occorre considerare il problema legato al diritto individuale di libertà, rispetto all'interesse pubblico collettivo che, come ho cercato di dire, non è sempre e solo legato alla sicurezza interna ed esterna, ma può essere connesso anche a molti altri aspetti.

Il sistema dell'*E-call* europeo, ad esempio, risponde all'interesse pubblico di diminuire il costo, in termini di vite umane ed economici, degli incidenti automobilistici. Tuttavia, può esservi un interesse pubblico anche maggiore a diminuire il costo di vite umane del personale dei servizi di sicurezza, dei servizi salvavita o di soccorso che sono tenuti a svolgere il proprio lavoro.

In definitiva, come vedete, si tratta di una materia complessa, che comporta dei tecnicismi incredibilmente sottili ma che rappresenta veramente un aspetto fondamentale della società che si sta costruendo intorno a noi.

PRESIDENTE. Do la parola ai colleghi che intendono intervenire per porre questi o formulare osservazioni.

ARNOLD CASSOLA. Professore, la ringrazio per la sua interessante esposizione.

Naturalmente, non possiamo che essere favorevoli a qualsiasi ampliamento di collaborazione, a livello civile, tra i vari Stati del mondo. Sul principio generale, quindi, credo che non ci siano problemi.

L'aspetto che in qualche modo mi preoccupa è legato alla frontiera, alla posizione *borderline* tra l'uso civile e non civile, alla definizione di ciò che è civile e

di ciò che non lo è. Dico questo, perché il trattato coinvolge tre Stati particolari, in cui probabilmente la definizione di che cosa sia la sicurezza e che cosa sia l'ordine pubblico differisce per motivi diversi.

Se prendiamo in esame Israele, ad esempio, avremo di fronte il caso di un Paese in guerra, che quindi avrà delle definizioni proprie delle finalità di uso civile o meno.

Per quanto riguarda gli Stati Uniti, credo che dopo l'11 settembre questi abbiano operato una profonda revisione della definizione di sicurezza, ordine pubblico e via dicendo.

Venendo alla Cina, anche questo Paese è molto lontano dalla nostra mentalità, per quanto riguarda la tutela dei diritti umani. Basti pensare al caso del Tibet. In questo momento, infatti, per una definizione diversa, non possiamo accogliere il Dalai Lama in Parlamento.

Mi preoccupa, quindi, capire quale tipo di tutela vi sia contro l'abuso o il cattivo uso delle informazioni, dei dati che vengono forniti e che vengono usati in maniera diversa.

Ad esempio, il rapimento di Abu Omar è stato operato usando proprio dei dati satellitari e verificando gli spostamenti di questa persona.

Chiedo, dunque, quali garanzie offrono questi trattati, affinché non vi sia un abuso dei dati che vengono trasferiti da Galileo ad altri sistemi.

Ho un'ulteriore curiosità, legata al fatto che, mentre nei titoli dei trattati per Israele e la Cina si fa chiaramente riferimento all'uso civile, per gli Stati Uniti, si parla di accordo concernente la promozione, la fornitura e l'uso di sistemi di navigazione satellitare, Galileo e GPS, e applicazioni correlate, senza menzionare la parola civile.

D'altra parte, tuttavia, nel testo c'è un riferimento continuo all'uso civile. Se non c'è il riferimento all'uso civile nell'accordo con gli Stati Uniti, non doveva esserci neanche in quello con la Cina e con Israele (*Commenti del deputato Pini*). Appunto, allora stiamo uscendo fuori dalle limitazioni civili.

Era una curiosità. Di tre titoli, due sono identici e l'altro non fa alcun riferimento all'uso civile.

GIANLUCA PINI. Ringrazio il presidente dell'Autorità garante. Mi scuso per il ritardo. Abbiamo voluto fortemente questa audizione, ma purtroppo la sovrapposizione con la scadenza della finanziaria, a maggior ragione per un piccolo gruppo parlamentare come il nostro, ci fa correre avanti e indietro per i vari palazzi.

L'esposizione del presidente Pizzetti è stata molto interessante e non retorica spesso e volentieri, infatti, si parla di trattamento di tutela, soprattutto dei dati personali, sensibili o non sensibili, con scarsa cognizione di causa. Per fortuna, la sua esposizione ci ha arricchito. In questo modo, nei prossimi incontri potremo intervenire sulle questioni specifiche con una maggiore conoscenza della materia.

Devo dire che parte proprio da chi vi parla la richiesta di questo tipo di audizione e di approfondimento, segnatamente per quello che attiene l'accordo con la Cina e Israele.

Il riferimento, dunque, non è rivolto tanto agli Stati Uniti che, lo ricordo al collega Cassola, fanno parte del Patto atlantico. Quindi, ci sono motivazioni molto diverse rispetto a quelle che riguardano la Cina o Israele, che hanno una situazione molto particolare.

Lo ripeto, non mi riferisco tanto agli Stati Uniti o a Israele, che dallo Stato italiano sono sempre stati considerati, anche in virtù dei trattati internazionali, degli alleati, ma al fatto di stringere accordi così delicati con un Paese che si chiama formalmente Repubblica popolare cinese, ma che di una Repubblica non ha assolutamente nulla.

Presidente, non so se lei sia mai stata in Cina. Si tratta di un Paese che, dal punto di vista dei diritti civili, non ha compiuto alcun passo in avanti, nonostante il periodo di Mao, nel quale si diceva che vi era stato il grande balzo in avanti in tale materia. Dall'epoca della

rivolta dei Boxer ad oggi, non si è sostanzialmente vista nessuna azione a tutela dei diritti dell'individuo.

Le domande che le rivolgo, dunque, riguardano proprio le garanzie che abbiamo come Paese che, con tutti i difetti possibili, cerca di garantire - e l'autorità che lei presiede ne è la prova - in qualche modo i diritti delle persone.

Le pongo alcuni quesiti, per poter capire meglio se è opportuno dare o meno l'assenso, anche se non determinante, a questo tipo di accordo.

Secondo la sua esperienza, quali sono i dati sensibili che, a seguito dell'accordo, potrebbero finire nelle mani - parlo schiettamente, come lei ha fatto fino adesso - del partito comunista cinese? Lo chiedo perché il partito comunista cinese è, di fatto, il Governo cinese. Vi è una sovrapposizione assoluta tra l'organo politico e l'organo governativo istituzionale.

Personalmente, lei si riterrebbe tranquillo, al sicuro, dopo aver visto il suo Paese siglare un accordo insieme agli Stati membri dell'Unione europea riguardo alla sua *privacy*, sapendo che, sul piano internazionale, è scarsissimo il livello di attenzione che la Repubblica popolare cinese rivolge non solo alla *privacy*, ma ai diritti umani in generale?

Questo è un aspetto importante, visto che lei presiede un'Autorità delicatissima. Infatti, se il presidente dell'Autorità garante si ritiene sufficientemente sicuro, anche per noi questo significa qualcosa; se invece c'è qualche dubbio, come noi riteniamo, vista la natura totalitaria del Governo della Repubblica popolare cinese, sarebbe sicuramente necessario fare approfondimenti più seri.

PRESIDENTE. Prima di dare la parola al professor Pizzetti, vorrei rassicurare l'onorevole Pini. Sono stata in Cina in occasione di una visita di scambio universitario. Ebbene, anche senza satellite, mi hanno dimostrato che sapevano tutto di me, in tutti i tipi di attività. Dopodiché, non ho voluto approfondire l'argomento.

GIANLUCA PINI. Presidente, lei sa che ho lavorato sei anni in quel Paese, quindi...

PRESIDENTE. Do la parola al presidente dell'Autorità garante per la protezione dei dati personali, professor Pizzetti, per la replica.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Pur sapendo di essere in Parlamento, quindi consapevole dell'oggettiva importanza di questa audizione, e anche dell'uso delle affermazioni che faccio, voglio essere molto esplicito con voi.

L'uso civile, come ho cercato di dire, comprende uno spettro amplissimo di attività possibili, che possono riguardare più o meno direttamente le persone.

Certamente, immaginare che nel mondo in cui viviamo, che ogni giorno di più assume un aspetto di integrazione e globalizzazione, sia possibile sottrarsi a questi nuovi sistemi di localizzazione satellitare è complesso.

Ho riportato l'esempio, apparentemente banale, ma anche molto concreto, di un uso molto frequente di questi sistemi di navigazione satellitare, connesso al trasporto merci via mare.

Non possiamo immaginare che tutte le navi in partenza, o destinate ad arrivare in un porto cinese, in ragione delle caratteristiche del Governo e del sistema giuridico di quel Paese, non debbano utilizzare questi sistemi, soltanto perché ciò potrebbe comportare la localizzazione dell'equipaggio. Poniamo, infatti, il caso che la nave abbia bisogno di aiuto, perché un membro dell'equipaggio ha avuto un incidente grave, e quindi deve essere localizzato da un servizio di soccorso che deve prendere il marinaio ferito per trasportarlo urgentemente in ospedale. Questo, peraltro, significherebbe anche conoscere un dato sensibile che attiene alla salute di un membro dell'equipaggio.

Ebbene, in ogni caso, credo che sia difficile rinunciare a questo tipo di servizio, soltanto in ragione del fatto che la nave parta o arrivi in un porto cinese. Ormai l'integrazione e l'utilizzazione di questi servizi, nel 90 per cento dei casi, comporta anche il trattamento dei dati delle persone che ne usufruiscono.

Siamo sempre più in presenza di cose che dialogano con le cose. Abbiamo anche chiarezza del fatto che i sistemi di geolocalizzazione consentono alle cose di dialogare tra loro.

Ovviamente, però, la cosa è legata anche a un uomo. Quindi, se una persona entra in metropolitana con un *badge* che contiene un RFID che dialoga con il sistema centrale che gestisce la rete metropolitana, comunicherà ovviamente l'ingresso in metropolitana del *badge*. Tuttavia, dialogando tra loro, le cose incidono anche sugli umani. Il sistema del cervello della metropolitana segnala che vi sono molti umani - usiamo questo termine da fantascienza, ma che è molto reale - che stanno accedendo al servizio e segnala ad un'altra « cosa », come il deposito dei vagoni della metropolitana, che sarebbe opportuno inserire un altro vagone nella linea. Certamente, vi potrà essere un conducente che riceve il segnale e sale sul vagone aggiunto, ma se il sistema di metropolitane è senza guidatore, come a Torino, il vagone potrà anche partire da solo.

In definitiva, dunque, si ha un *badge* che entra in metropolitana e dialoga con un cervello che, a sua volta, comunica con il vagone della metropolitana che può anche partire in automatico, senza neppure bisogno di un conducente. Tuttavia, viene aggiunto un treno di carrozze sulla linea, perché ci sono molti umani sulla banchina. Il fatto che queste « cose » dialoghino fra loro ha una indubbia utilità per i passeggeri. Sono state pensate e progettate per arrecare vantaggi agli stessi.

A questo punto, se rinunciamo a tali prospettive, avendo paura che le « cose » dialoghino, dobbiamo essere consapevoli che rinunciamo anche ad avere un vantaggio: nel caso sopra citato i passeggeri potrebbero aspettare meno sulla banchina della metropolitana ed avere carrozze meno affollate.

Lo stesso vale per i sistemi di geolocalizzazione e di navigazione satellitare. Vi sono « cose » che dialogano con altre « cose » che, tuttavia, riguardano anche gli umani.

Peraltro, probabilmente, nel 90 per cento degli eventi normali, gli umani non lo sanno neanche. Tutto funziona in automatico.

Certo, ragionando su tali argomenti, dobbiamo sempre aver presente che questi sistemi, che noi costruiamo e che producono vantaggi, possono implicare anche forme di controllo su di noi. Pertanto, occorre pensare in modo laico che si tratta di servizi civili che, in quanto tali, sono legati all'uomo e che possono riguardarlo anche in attività legate a dati sensibili. È chiaro che se una persona si ammala e arriva l'elicottero per portarla via, tutti sapranno che l'individuo in questione è ammalato. Tuttavia, il servizio è stato creato apposta per quel motivo.

Detto questo, tenendo presente che la nave che gira per il mondo entra sotto la sovranità di un certo numero di Paesi, posso rifiutare tale realtà, perché tra questi Paesi vi è la Cina?

Del resto vi potrebbe essere un Paese anche peggiore della Cina. Questa è la realtà in cui viviamo e che ci obbliga ad essere realisti. Altrimenti, definiamo una realtà che immaginiamo di padroneggiare più facilmente con le nostre categorie tradizionali.

Quindi, quando parliamo di usi civili — l'onorevole Cassola giustamente vi ha fatto riferimento in relazione alla Cina — dobbiamo avere chiare queste implicazioni.

Occorre tenere inoltre presente che il dato sensibile è sempre « in agguato ». Vi sono, infatti, diverse informazioni di carattere sensibile, relative ad esempio a specifiche patologie, che possono riguardare una persona. Dialogando tra di loro, le « cose » possono registrare tali informazioni, e una persona capace di analizzare i dati registrati può avere la possibilità di dedurne anche informazioni sui dati sensibili.

Poiché, casi di questo genere possono essere potenzialmente numerosi, rischiano di farci rinunciare alle opportunità che le tecnologie ci possono offrire.

Riporto un esempio, magari banale, ma possiamo immaginarne anche altri.

Poniamo il caso di una persona che entra in metropolitana con l'RFID, che consente una serie di facilitazioni. Potrebbe risultare che tutti i venerdì alla stessa ora, la persona entra in una certa stazione della metropolitana ed esce in un'altra che, guarda caso, è quella della moschea di viale Jenner a Milano. Ebbene, è probabile che un attento analista — sulla base dei dati raccolti in automatico — possa immaginare che l'abbonato, possessore di quel *badge*, non sia solo un musulmano, ma anche un osservante. Infatti, alla stessa ora, tutte le settimane, in modo ripetitivo, rituale, egli arriva a quella determinata uscita della metropolitana che si trova vicino alla moschea. Quindi, si può presumere, come indizio, che probabilmente quell'individuo è un osservante musulmano. In questo modo, dunque, si individua un dato sensibile, quale quello relativo alla religione.

Per evitare questo rischio, devo rinunciare alla tecnologia RFID, ossia al *badge* con il quale entro agevolmente e rapidamente in metropolitana? La questione è molto delicata.

Se entrate a fondo nella materia, vi renderete conto del fatto che è difficilissimo capire come conciliare in concreto i valori, le norme che abbiamo scritto e a cui vogliamo rimanere fedeli, e le nuove tecnologie.

Voglio entrare ancora di più nello specifico della questione, perché giustamente l'onorevole Cassola ha sottolineato l'aspetto legato ai problemi di sicurezza.

Anche in questo caso voglio essere molto franco, dicendo che persino all'interno della Comunità europea la nozione di sicurezza cambia da Paese a Paese.

Pensiamo a un cittadino italiano che si reca in Inghilterra. Con tutte le normative esistenti e tutto ciò di cui si sta parlando, per quanto riguarda l'uso dei dati di navigazione satellitare, ai fini di sicurezza, si entra nel sistema inglese. Occorre, dunque, considerare il concetto di sicurezza che si ha in Inghilterra che, come è noto, è molto condizionato dal terrorismo irlandese.

Mi è stato chiesto se mi sentirei certo e tranquillo andando in Cina. Posso rispondere, chiedendo all'onorevole Pini che mi ha posto la domanda, se si sentirebbe ugualmente tranquillo.

GIANLUCA PINI. Non le ho fatto questa domanda.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Potremmo dire che ci sentiamo tutti tranquilli, con lo stesso livello di tranquillità, in tutti i Paesi dell'Unione europea, quando entriamo in contatto con concetti di sicurezza diversi?

Questo è uno dei motivi, per cui per noi è importante anche l'integrazione europea dei sistemi di sicurezza, la quale però pone problemi ancora più delicati, in materia di controllo effettivo dei dati.

Del resto, posso sentirmi più tranquillo se ho delle categorie comuni, condivise da tutti i Paesi europei, ma mi interrogo su quale sia il grado di effettività di questa normativa.

Siamo sicuri che l'effettività, non quello che c'è scritto nelle leggi, sia uguale in Lituania, in Macedonia, in Romania, in Italia e in Spagna?

Tra l'altro, dovete sempre tener presente che man mano che ci spostiamo all'interno dell'Unione europea, anche ai fini di protezione dati, entriamo sotto i regimi dei diversi Paesi in cui ci rechiamo, non rimaniamo sotto il nostro ordinamento. Lo stesso vale per gli altri quando entrano in Italia.

Infine, posso dirvi che non abbiamo chiaro, anche in termini giuridici, che cosa siano le finalità di sicurezza e di giustizia nemmeno in Italia?

L'articolo 53 della legge sulla *privacy*, in vigore dal 2004, prevede che il Ministero della giustizia e il Ministero dell'interno indichino, con appositi decreti ministeriali, le banche dati, in possesso delle due amministrazioni, gestite per finalità di giustizia e sicurezza. Ovviamente, ciò deve avvenire contemporaneamente, per definire in modo ufficiale che cosa sia l'attività di sicurezza e che cosa sia l'attività di

giustizia: ebbene, i decreti non sono stati emanati.

Quindi, se mi si chiedeste quante sono le banche dati operanti in Italia a fini di giustizia e sicurezza, dovrei rispondere che non lo so.

A quel punto, con assoluta ragionevolezza, mi si potrebbe domandare come faccio a svolgere il mio mestiere. A tale quesito, risponderei che sono due anni che, nella relazione al Parlamento, sollecito la predisposizione di questi decreti.

Quando vado a verificare il trattamento dei dati del DNA da parte di alcuni reparti dei RIS dei carabinieri, so come agire, perché un ricorso mi ha messo sull'allarme per tale questione. Tuttavia, non dispongo di un elenco ufficiale delle banche dati, ai fini di giustizia e sicurezza, che i due Ministeri e le due amministrazioni utilizzano. Quindi, come vedete, il tema è molto complesso.

Volutamente, consapevolmente e responsabilmente sto ampliando le mie risposte, al di là delle vostre domande, proprio perché voglio cogliere questa occasione anche per chiedere l'aiuto del Parlamento, affinché sia possibile avere finalmente l'attuazione dell'articolo 53 del codice in materia di protezione dei dati personali, vigente in Italia dal 2004.

GIANLUCA PINI. Presidente, non ho avuto risposta a una domanda specifica.

PRESIDENTE. Forse neanche l'onorevole Cassola.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Il quesito dell'onorevole Cassola lo ricordo e rispondo subito. Per quanto riguarda l'onorevole Pini, se possibile, vorrei invitarlo a riformulare la domanda...

PRESIDENTE. Va bene. Allora, onorevole Pini, ponga di nuovo sinteticamente la domanda. Mi preme semplicemente far intervenire tutti, perché sento un grande interesse per l'argomento in questione.

GIANLUCA PINI. Certo. Si tratta di un interesse che non c'era, fintanto che l'op-

posizione non ha stimolato il dibattito su un argomento che doveva passare in due minuti in Commissione. Le cose vanno dette come stanno.

EMILIA GRAZIA DE BIASI. Direi che si viene per tempo e si ascolta quello che dice il presidente!

PRESIDENTE. Scusate, siamo in sede di audizione, non facciamo una polemica sciocca...

GIANLUCA PINI. Presidente, se mi reco in Cina, o in un Paese dove so che le garanzie relative ai diritti civili, individuali o alla *privacy* sono molto più labili di quelle esistenti nel mio Paese, sono consapevole di mettermi in una condizione di debolezza. In quel caso, però, scelgo autonomamente e personalmente di recarmi in un Paese o di trattare da un punto di vista commerciale con la Cina, piuttosto che con il Vietnam, o con gli Stati Uniti.

Tuttavia, l'accordo stipulato tra l'Unione europea - della quale l'Italia è uno Stato membro, anzi fondatore - e la Cina prevede, all'articolo 6 del trattato, ad esempio, che il centro di ricerca abbia sede a Pechino.

Con la mia domanda, le chiedo se si sente tranquillo in casa sua, rispetto ai suoi dati, ai suoi spostamenti in Italia. Del resto, lei vive in questo Paese, è cittadino italiano.

Nel momento in cui si decide di creare a Pechino un centro di ricerca che deve sviluppare una piattaforma comune - relativamente a queste cose, che dialogano con altre cose, come giustamente le chiama lei -, si sente tranquillo del fatto che qualcuno, in Cina, a sua insaputa, senza che lei coscientemente scelga di avere a che fare con i cinesi, spinga un bottone e possa accedere alle sue informazioni, mentre lei si trova a casa sua?

PRESIDENTE. Presidente Pizzetti, sono state poste delle domande, di cui una specifica, sui trattati e sulle nostre ratifiche. Lo sottolineo, perché credo che ci sia un effettivo interesse in proposito, non solo da parte dell'opposizione.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. L'argomento è così tecnico e, come avrete capito, sono mosso da una passione tale che posso fare involontariamente confusione.

Come ufficio - peraltro, il segretario generale è presente in aula -, possiamo rispondere alla domanda posta, dicendo che Galileo è semplicemente un sistema di ripetitori che non comporta archiviazione, ritenzione, e conoscibilità dei dati.

Per quello che riteniamo di leggere nell'articolo 6 del trattato, il centro di ricerca di cui lei parla, onorevole Pini, è finalizzato all'integrazione dei sistemi satellitari e non al loro uso.

Quindi, il trattato, così com'è configurato, non riguarda l'uso che sarà fatto di questi trasmettitori. Allo stesso modo, quando parlo di servizi civili possibili, mi riferisco al trasmettitore che è costruito per poterli fornire, ma non è il sistema Galileo che li eroga.

Insomma, una volta installate le parabole, non sono queste che trasmettono i programmi di Sky o di altro tipo.

Quindi, il sistema di integrazione con la Cina ha un carattere tecnico rispetto alle modalità di organizzazione di questo sistema satellitare, al fine di fornire successivamente quei servizi.

Sarà in quel momento, rispetto a quel tipo di attuazione ed eventuale integrazione, o non integrazione, tra i diversi titolari dei servizi, nei differenti Paesi, che la sua domanda avrà perfettamente ragione non solo di essere posta, ma anche di essere approfondita.

PRESIDENTE. Do la parola ai colleghi che intendano porre ulteriori domande.

EMILIA GRAZIA DE BIASI. Ringrazio il presidente Pizzetti per averci spiegato che gli accordi sono di contenuto tecnico, riguardano l'interoperabilità, non coinvolgono il trattamento di dati personali, per cui da questo punto di vista non c'è nessun rilievo. Dico questo per motivi di chiarezza rispetto al nostro lavoro.

Pertanto, quella di oggi è un'audizione - per me, personalmente, che mi occupo

di questo settore - di straordinario interesse, ma che meriterebbe persino di essere allargata ad altri aspetti non attinenti alla materia che stiamo trattando nella nostra funzione consultiva.

Penso, dunque, che possiamo anche permetterci, così come ha fatto il presidente Pizzetti, di allargare un pò il campo del ragionamento.

Ritengo che le obiezioni che sono state mosse non abbiano a che fare esclusivamente con il tema della *privacy* e della trattazione dei dati personali, ma siano legate alla politica estera di un Paese - mi pare che questo sia un tema ben più ampio di quello che stiamo esaminando oggi -, al tipo di relazione che deve intercorrere tra gli Stati e a quale deve essere la capacità di azione di un soggetto politico, ossia l'Europa, nei confronti di altre nazioni.

Da questo punto di vista, dunque, vedo una differenza di fondo, che però non ha a che fare immediatamente con il tema che stiamo trattando oggi.

Il punto della discussione che mi interessa molto è quello relativo al rapporto tra sicurezza e libertà.

Ritengo che la libertà, come è ovvio, comporti dei rischi individuali e collettivi, e credo anche che le tecnologie comportino dei rischi sul piano del rapporto con la libertà individuale.

D'altra parte, però, penso che sia necessario compiere una scelta di fondo. Dobbiamo decidere se vogliamo un mondo che coopera, oppure che costruisce muri.

Questo è ciò che ritengo (*Commenti del deputato Pini*)... Onorevole Pini, la pregherei di avere tutta la considerazione necessaria per concezioni che sono molto diverse. Vorrei che la smettesse con queste sceneggiate. Dobbiamo fare il teatrino tutte le volte!

Le questioni che volevo porre al professor Pizzetti sono due, anche se sarebbero molto più numerose.

La prima domanda è legata ai problemi relativi all'interoperabilità, che mi sembrano considerevoli, dal punto di vista della capacità tecnologica di ciascun sog-

getto, non esclusivamente sul piano del codice dell'azione, ma dell'investimento che si fa in origine.

Visto il sistema Galileo e l'iter molto travagliato che ha avuto il finanziamento del progetto Galileo, l'Europa riesce ad avere una parità tecnologica rispetto agli altri Paesi, segnatamente gli Stati Uniti e la Cina?

Sappiamo che la Cina è molto più avanti di noi, per quel che riguarda la capacità di controllo di Internet, ad esempio. Come è ovvio, questo non ha nulla a che vedere con i satelliti. Esiste una linea di sviluppo tecnologico che nasce in modo differente, quindi con finalità militari, ma ciò che mi chiedo è se l'Europa ha questa capacità di controllo tecnologico paritario o se rischia di essere fagocitata dagli altri sistemi.

Il secondo quesito che le pongo riguarda i minori. Si tratta di un problema che oscilla tra esigenza di tutela e violazione dei diritti individuali. Ciò che mi impressiona molto è l'attuale incapacità di trovare un punto di equilibrio, rispetto alla determinazioni europee e internazionali, per la tutela dei minori nell'uso delle tecnologie.

Si è discusso di tale argomento con il dottor Calabrò, in sede di VII Commissione, per quel che riguarda una proposta di legge sulla tutela dei minori rispetto ai film e ai videogiochi.

Credo che oggi non sia più l'epoca di parlare di comune senso del pudore. Occorre riflettere su un argomento più profondo. Mi riferisco al fatto che i minori utilizzano, a partire da un'età precocissima, strumenti rispetto ai quali non abbiamo capacità di controllo, perché i filtri mostra a nostra disposizione sono assolutamente banali.

In questo caso, dunque, la domanda è inversa. A suo parere, quali sono le scelte che vanno fatte per salvaguardare la libertà, ma contemporaneamente per consentire una tutela del minore rispetto all'accesso alle informazioni, che è un punto piuttosto determinante?

Invece, ciò che lei, presidente Pizzetti, diceva - mi permetta solo una battuta -

a proposito dei minori e della possibilità di avere un braccetto con il controllo satellitare, mi auguro che non succeda mai. Una volta, mia sorella si è persa in uno stabilimento balneare, ma è bastato camminare un pò per trovarla.

Mi impressiona molto che sui minori possa esserci un eccesso di controllo, che porta, a mio avviso, a una deresponsabilizzazione rispetto alla libertà individuale.

ANGELO PICANO. Vorrei porre due domande e svolgere un'osservazione.

Vengo alla prima domanda. Man mano che il tempo passa, siamo invasi sempre più da messaggi commerciali che ci arrivano sul telefono o attraverso le *e-mail*. Qualcuno suggerisce di limitarsi a rispondere - nel caso delle offerte commerciali telefoniche - di non essere interessato. Intanto, però, devo rispondere e, se sono una persona gentile, non chiudo la comunicazione, ma quantomeno cerco di far capire che non è il caso di insistere. Tuttavia, se fatti del genere cominciano a verificarsi più volte al giorno, diventano un fastidio notevole, che finisce per creare delle serie preoccupazioni.

Lo stesso discorso vale per le *e-mail*, dalle quali siamo letteralmente invasi. Se il destinatario ha la curiosità di aprirle, perde tempo, oltre al fatto che, qualche volta, ci si può imbattere anche in un messaggio capzioso.

Mi chiedo, dunque, se sia tecnicamente possibile fare in modo che all'arrivo di un messaggio commerciale sul telefono corrisponda un suono diverso; oppure se sia possibile obbligare coloro che inviano messaggi commerciali tramite *e-mail* a introdurre una sigla, in modo che il destinatario sappia di che tipo di comunicazione si tratta, e quindi abbia la facoltà di ignorarla.

L'osservazione che volevo svolgere, invece, riguarda un altro aspetto. Sebbene sia stata messa in piedi un'architettura mastodontica, a livello universale, sulla difesa della *privacy*, i contenuti delle conversazioni telefoniche vengono sbattuti tranquillamente sui giornali, in ragione del diritto di cronaca e di informazione, e

divengono oggetto di processi. Non ho mai visto, tuttavia, che il Garante della *privacy* sia intervenuto in maniera ferma, chiedendo l'adozione di provvedimenti giudiziari, come il sequestro o l'interdizione dalla pubblicazione di queste conversazioni. Sembra quasi una barzelletta: qualsiasi cosa si dica, dopo un breve periodo finisce sui giornali. Che provengano dall'autorità giudiziaria o da qualsiasi altra fonte, le conversazioni private vengono sbattute in prima pagina, con le conseguenze che ne derivano.

Infine, vorrei sottolineare - perché ne rimanga traccia agli atti - che applichiamo alle conversazioni private, in cui il soggetto che parla è portato a essere più libero nelle sue espressioni, la stessa morale e lo stesso rigore giuridico che riserviamo alle conversazioni pubbliche.

Questo è un problema su cui occorre riflettere. Del resto, un conto è, stando a casa mia, giudicare - nel bene e nel male - il comportamento di una certa persona; altro conto è farlo in pubblico, dove è necessario un maggiore *self-control*.

PRESIDENTE. Credo di esprimere il sentimento, se non la volontà della Commissione, dicendo che il presidente Pizzetti dovrà tornare in Commissione per un ulteriore incontro.

GABRIELE FRIGATO. Ringrazio il dottor Pizzetti per la sua presenza, per le cose che ci ha detto e anche per l'orizzonte che è riuscito ad aprire in me, rispetto a queste tematiche che, obiettivamente, sono tanto complesse, quanto spesso non sufficientemente affrontate in sede politica e istituzionale.

Il fatto che, come veniva ricordato, da qualche anno ormai si registri un ritardo nell'emanazione dei decreti attuativi - se non ho capito male - basta a segnalare quanto tale attenzione abbia bisogno di essere rafforzata, e quindi di trovare concretezza.

Mi spiace che il collega Pini sia andato via; mi pare peraltro che, quando abbiamo immaginato questa audizione, sostanzialmente, siamo partiti dall'articolo 6 del

trattato con la Cina e dalla localizzazione di un centro di studio e ricerca a Pechino, di cui proprio l'onorevole Pini parlava in precedenza. Mi sembra che la risposta fornita ai quesiti relativi a tali temi rassereni rispetto alle nostre preoccupazioni. Quando poi si tratterà, eventualmente, di localizzare dei punti di raccolta e tenuta dei dati, qualche riflessione in più certamente bisognerà svolgerla.

Già in una precedente seduta abbiamo parlato di questo argomento. Sapevamo, infatti, che in questa materia sconfiniamo dalle competenze di questa Commissione, dalle valutazioni concrete e sostanziali del provvedimento, addentrandoci nei rapporti che il nostro Paese intrattiene con l'Unione europea, che questa ha con gli altri Paesi, che l'Italia ha con la Cina, e via dicendo.

Indubbiamente, quindi, non poteva e non può essere questa la sede per avere tutti i chiarimenti necessari in tale materia. Tuttavia, dal momento che qualche collega vi ha fatto riferimento, penso sia giusto ricordare che qualche anno fa erano più numerosi i Paesi che, per quanto riguarda il tema delle libertà e della democrazia, preoccupavano nei dibattiti in Italia e nell'Europa occidentale. Alludo a ciò che è successo in quello che viene definito impero sovietico, o l'europa orientale.

Oggi, in tale quadro, qualche passo in avanti è stato fatto, anche che se le ultime notizie rispetto ad alcuni atteggiamenti del Presidente Putin non ci rassicurano molto. Dico questo perché certamente non si può essere sereni rispetto alla mancanza, in Cina, della tutela dei diritti umani, di regole certe e della libertà (e potremmo continuare questo elenco).

Sicuramente, quindi, dobbiamo avere una serie di attenzioni, proprio perché credo che nel difficile rapporto - che anche quest'oggi il presidente Pizzetti sottolineava - tra il quadro delle libertà e quello della sicurezza, le nuove tecnologie debbono essere al servizio equilibrato di questi due valori. Nell'ambito di tale ricerca, neanche noi abbiamo trovato un punto di sintesi finale. Nel momento in cui

ci relazioniamo con Paesi che hanno qualche difficoltà in più rispetto a questi temi di questi diritti, l'attenzione deve essere sicuramente maggiore.

In tale quadro, credo che non possiamo rifiutare un rapporto neanche con i Paesi più chiusi. In nessun caso possiamo immaginare che il dialogo ed il confronto non siano lo strumento principe di relazione. Quindi, anche nei confronti della Cina, credo che l'Italia e la Comunità europea abbiano il dovere di portare avanti un'azione continua di sollecitazioni e di indirizzo. D'altronde, sappiamo tutti che la Cina è un grandissimo Paese in movimento che, probabilmente, in campo economico, ha conosciuto la libertà, ma non ha fatto altrettanto sul piano dei diritti delle persone e dell'organizzazione dei rapporti.

Se fosse stato presente il collega Pini, avrei aggiunto una riflessione, che lascio semplicemente agli atti. A mio avviso, non possiamo essere preoccupati per le chiusure. È giusto che ci preoccupiamo della chiusura di qualunque Paese, ma mi sarebbe piaciuto poter valutare alcuni atteggiamenti di chiusura con il collega Pini anche alcuni atteggiamenti di chiusura in qualche cittadella veneta stanno avvenendo rispetto a problemi specifici. Tuttavia, dal momento che l'onorevole Pini è assente, è inutile che prosegua questo ragionamento.

Concludo con una curiosità. Il presidente Pizzetti, in precedenza, metteva in relazione il valore del consenso con il valore della consapevolezza, proprio attorno a questi temi. Ho l'impressione che questo sia un rapporto da ritrovare, in questi termini, su molte tematiche. Forse, è la sfida della democrazia del nuovo secolo, del nuovo millennio, sulla quale non sarà facile trovare la complementarietà di questi due elementi.

Restando ai temi che di cui lei, presidente Pizzetti, ci parlava, l'impressione è che oggi - parlo per me, non voglio assolutamente coinvolgere nessun altro - ci sia una maggiore consapevolezza rispetto ad alcuni temi, sui quali dovrà esserci, eventualmente, una presa di posi-

zione e quindi un consenso. Proprio in riferimento a questa consapevolezza, credo che l'audizione odierna sia stata proficua.

PRESIDENTE. Prima di dare la parola al presidente Pizzetti, vorrei riprendere l'ultima notazione dell'onorevole Frigato, che ha parlato dell'attività di questa audizione, considerato che, quando formuliamo pareri al Governo o alle altre Commissioni, spesso non abbiamo gli strumenti della consapevolezza.

Partendo da questo dato, vorrei sottolineare alcuni temi. Del resto, abbiamo allargato molto l'ambito della discussione - il presidente risponderà come ritiene -, perché dobbiamo continuare ad attirare i temi dalla nostra parte, sul *côté* europeo.

Molto spesso, quando esprimiamo pareri alle altre Commissioni e al Governo, tornano alcuni temi di fondo, su cui non consideriamo il quadro della normativa europea. Dovremmo invece utilizzare audizioni come quella odierna a questo scopo.

Pertanto, ho stilato un elenco di temi rispetto ai quali sarà molto utile incontrare nuovamente il Garante. Il primo tema riguarda la tutela della *privacy*.

Molto spesso, esprimiamo pareri su temi di fondo rispetto ai quali sarebbe opportuno audire oltre che il Garante della *privacy*, anche altri soggetti. Potrà trattarsi, forse, di incontri non necessari nello specifico dei temi, ma utilissimi per inquadrare i nostri pareri nel *framework*, nel contesto della normativa europea e nel rapporto tra questa e la normativa, per quanto riguarda la *privacy* e la sicurezza.

Abbiamo espresso una serie di pareri sul danno biologico, ma il tema del differente valore della vita umana è assolutamente presente nelle considerazioni del presidente Pizzetti.

Quanto al tema del rapporto fra consenso e consapevolezza, ovviamente, da questo punto di vista si pone il problema delle asimmetrie di informazione, legate a varie differenze di competenze. Per quanto mi riguarda, ad esempio, non sapevo che cosa fosse l'RFID, per cui rispetto a questo mi dichiaro incompetente.

In una popolazione che invecchia, dunque, si pone il problema di capire come si articola il rapporto fra consenso e consapevolezza, tematica che spesso ricorre, per esempio, nel campo della salute. Non sappiamo - o almeno, non so - se esiste un quadro di normative europee sul consenso informato. In questo caso, non sappiamo se ci sono degli obblighi europei - domanda che pensavo formulasse l'onorevole Cassola - nell'uso del sistema satellitare o di altri tipi di comunicazione, come « salvavita », in presenza di cittadini comunitari o non comunitari in pericolo (abbiamo espresso pareri sulle direttive relative al controllo dei mari).

Ci sono degli obblighi o non ne discende alcuno, perché manca l'integrazione tra sistemi di sicurezza e non so cos'altro? Quanto agli obblighi nei confronti del cittadino comunitario, mi chiedo su chi gravino le spese, e via dicendo.

Per ovvi motivi, quindi, gli accordi in questione sono simili, ma anche molto diversi tra loro. Nell'accordo relativo agli Stati Uniti, si parla di una volontà europea, di un sistema globale autonomo europeo di misurazione del tempo e di navigazione satellitare. Dunque, vi sono delle regole comuni rispetto alla definizione di Galileo. Mi chiedo, tuttavia, se per le restanti regole - penso, ad esempio, alla sicurezza - si segue un'altra strada.

Ci sono dei temi, di pertinenza della nostra Commissione, rispetto ai quali dovremmo avere una conoscenza che va al di là del singolo parere, perché ci servono per moltissimi altri pareri.

Pertanto, mi riservo di proporre di svolgere su determinati temi, non solo l'audizione del Garante, ma anche audizioni di altri soggetti interessati alle questioni in esame.

Tra gli altri temi, abbiamo parlato anche di quello riguardante il mare. Mi chiedo se in proposito esiste o meno qualche obbligo, oppure se tale tema appartiene a regole di consuetudine internazionale, condivise o meno.

Spero, presidente, che non le abbiamo posto troppe domande che esulano da

parte mia, dalle sue competenze; ho cercato di riportare i quesiti nel quadro delle normative europee.

Do la parola al presidente Pizzetti per la replica conclusiva.

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Presidente, mi ha posto delle domande che mi sollecitano terribilmente, anche nel mio mestiere « normale », che è quello di studioso dei sistemi costituzionali, quindi cercherò di contenere l'entusiasmo.

Direi che il suo ultimo intervento è di interesse estremo, per una riflessione sulla democrazia moderna e il ruolo del Parlamento. Non c'è dubbio, infatti, che viviamo in una realtà, anche a prescindere dalle tecnologie di cui stiamo parlando, sempre più complessa, con un livello sempre più elevato di norme tecniche e di tecnicismi.

Questa democrazia, quindi, immaginata per un mondo molto più semplice - in cui l'opinione pubblica era informata attraverso la cultura stessa, le organizzazioni politiche e i grandi movimenti operai e sociali dell'ottocento -, era in grado di padroneggiare la realtà.

Inoltre, i Parlamenti che attraverso la rappresentanza erano capaci di esprimere queste consapevolezze, proprio perché ognuno era in grado di padroneggiare la realtà, ora, di fronte a questo incredibile e rapido sviluppo tecnologico, sono in grande difficoltà.

Presidente, lei ha toccato esattamente il tema più solido e radicato di fronte al quale ci troviamo. Non a caso ho usato i termini consenso e consapevolezza - mi fa piacere che siano stati ripresi -, poiché trattano un tema che voglio sviluppare più volte nel prossimo futuro.

Certo, esiste il consenso. La *privacy* vive di consenso e di informazione, ma ci scontriamo con questa realtà che vorrei spiegarvi, in sintesi, sotto due profili.

L'informativa, che le nostre leggi richiedono quando si fa uso di dati personali, è innanzitutto - e bisogna capirlo, perché ha un senso - finalizzata ai tecnici del diritto. Attraverso l'informativa, vi devo

informare (io, in quanto ipotetico titolare di un trattamento di dati) di tutti i vostri diritti e del modo con cui userò i vostri dati, secondo modalità tali per cui, se domani vengo citato in giudizio, posso dimostrare al giudice che, ai sensi del diritto vigente, vi ho fornito tutte le informazioni necessarie.

La realtà di questa società, in questo momento storico, è che quando il Garante afferma che occorre informare i cittadini dell'uso che si farà dei loro dati, invita a dare un'informativa di tipo giuridico, pensata avendo a mente il contenzioso civile o penale davanti a un giudice. Questo è il motivo per cui capita spesso di trovare informative illeggibili.

Pertanto, se vi recate in banca, vi chiedono di porre la firma relativa alla *privacy*, in calce a un modulo che ha le dimensioni per lo meno di una pagina e, per di più, scritta in piccolo. Per comprendere quel testo, non basta avere una laurea in legge, ma occorre anche una specializzazione, in quel caso di diritto civile, o di diritto bancario, e un master in protezione dei dati personali.

Un'informativa di questo tipo se è corretta dal punto di vista giuridico, non ha alcuna utilità sotto il profilo della consapevolezza del soggetto che la legge. Serve unicamente ad accrescere l'antagonismo del cittadino verso la protezione dati.

Il problema è che, da un lato, quella informativa ha una sua ragione d'essere; dall'altro non mi garantisce la consapevolezza. Tuttavia, la consapevolezza diventa sempre più essenziale man mano che ci spostiamo dalle realtà note a quelle nuove.

La nostra esperienza, infatti, ci dice - e viviamo tutti liberamente, anche chi non ha mai studiato diritto - che se si compra un libro, si ha diritto ad avere il libro. Inoltre, se il libro ha dei difetti, perché ci sono pagine non stampate, ho la possibilità di farmene dare un'altra copia. Dopodiché, arriva l'avvocato che spiega in quale casella giuridica del rapporto contrattuale si trova tutto questo, definisce quali sono i vizi del contratto e via dicendo.

Io sono però già consapevole, grazie anche agli insegnatami che mia madre mi

ha trasmesso fin da piccolo, del fatto che se compro una cosa, ho diritto ad averne una corrispondente a quella per la quale ho dato il denaro.

Quando vengo in contatto con le nuove tecnologie, entro in un mondo in cui la consapevolezza è essenziale, perché nessuno ci ha insegnato che cosa significa inviare una *e-mail*. Nessuno ci ha mai detto che una *e-mail* è sostanzialmente una cartolina aperta.

Se spedisco una cartolina, so che la portinaia o il portalelettere la possono leggere; se voglio evitarlo, metterò la cartolina in una busta chiusa; se voglio che sia ancora più protetta, la invio tramite raccomandata con ricevuta di ritorno.

Quando invio una *e-mail*, nel mio immaginario, spedisco un messaggio segreto. Del resto, mando una *e-mail* da casa mia ad un'altra persona che la legge a casa sua. Quindi, tutto penso, tranne che sia una cartolina aperta che milioni di persone, se hanno le tecniche adatte, possono leggere. Questo è quello che intendo per consapevolezza.

Non mi interessa che Yahoo, Google, Microsoft o Tiscali, quando si vuole aprire una casella di posta elettronica, inviino tre videate per la *privacy* e invitino a cliccare per il consenso, pena la mancata fornitura del servizio. Tutti, alla terza riga, fanno scorrere la videata, cliccano e hanno il servizio senza aver letto e capito niente. È questo quello che intendiamo per consapevolezza?

Le nuove tecnologie, dunque, richiedono uno sforzo enorme da parte di tutta la società.

Un problema che citava l'onorevole De Biasi riguardava l'insegnamento ai giovani in tale settore. Prima di tutto, occorre capire che cosa si deve insegnare, perché non lo sappiamo neanche noi.

Ci troviamo di fronte all'ignoranza dei fenomeni, per cui siamo certi dei nostri valori, ma non sappiamo come questi devono declinarsi in una realtà che ci è ignota.

Molto banalmente, posso portarvi il caso di YouTube e dei filmati di quello che succede nelle classi scolastiche. Non co-

nosco la vostra esperienza scolastica. Per quanto mi riguarda, nel corridoio del liceo Plana ad Alessandria, durante l'intervallo, fra ragazzi facevamo la lotta libera, ci buttavamo a terra, ci tenevamo in piedi, ci facevamo gli scherzi, ci rubavamo la merenda l'uno con l'altro.

Se qualcuno avesse trasmesso questi episodi su YouTube e avesse mandato il filmato in onda al telegiornale della sera, quella sarebbe sembrata una scuola drammatica.

Con questo, intendo dire che gli stessi fatti cambiano dimensione, in virtù del mezzo tecnologico. Adesso, ci troviamo in una situazione drammatica.

A volte ci ritroviamo, con il compagno che buttavo sempre per terra e, scherzando, ricordiamo quei tempi. Se quelle immagini fossero ancora visibili, danneggerebbero enormemente la nostra attività professionale.

Il Garante inglese ha appena concluso un'attività di indagine, con la quale ha dimostrato concretamente che le immagini presenti su YouTube, o quelle che entrano in rete, sono utilizzate dai datori di lavoro per profilare le persone che fanno domanda di assunzione. Pertanto, basarsi su comportamenti disdicevoli avuti da ragazzini, può diventare un elemento per cui non si è assunti.

Per questo motivo, dico che non mi basta il consenso, ma voglio la consapevolezza.

È inutile spiegare ai ragazzi che inviare i filmati registrati con il proprio telefonino a YouTube significa dare il consenso.

È spaventosamente difficile spiegare tutto questo, perché abbiamo a che fare con tecnologie complesse e continuamente in fase di sviluppo (avete visto, già stamattina, le difficoltà a cui siamo andati incontro).

Anche per quanto riguarda i minori, di cui si è parlato in precedenza, la questione è complessa. Probabilmente, l'onorevole De Biasi ha un livello molto alto di protezione della responsabilità genitoriale.

Per evitare lo scambio di neonati in una clinica di maternità, invece di mettere il braccialetto alla caviglia, che può essere

anche scambiato, si può usare una RFID, ossia un *chip*. In molte cliniche viene fatto, ma è un'operazione delicata, perché tocca valori molto complessi.

Devo dire anche che personalmente, come Autorità, sento molto questo problema. Queste Autorità ipertecniche, infatti, sono spesso chiamate ad assumersi la responsabilità di decidere, in nome della collettività, cosa è giusto e cosa è sbagliato, dove occorre alzare il livello di protezione dati e dove invece è necessario cedere spazio alle esigenze di sicurezza.

Personalmente, non me la sento di giudicare in merito. Posso rappresentare al mio Paese i termini della questione, ma posso essere certo di decidere sempre, senza contatto con il mio Parlamento, mantenendo la mia indipendenza e lavorando con gli altri Garanti dei Paesi europei?

Possiamo noi, solo perché abbiamo più competenze tecniche e più specializzazioni, sostituirci a un giudizio di valore che riguarda una società? Per essere in contatto con questa, abbiamo bisogno che riunioni come queste si moltiplichino, affinché il Parlamento possa anche essere coinvolto.

Venendo alle domande specifiche, devo una spiegazione puntuale all'onorevole Cassola e all'onorevole Pini.

Onorevole Pini, per noi la risposta è sicura. Il centro di ricerca riguarda il sistema satellitare, non il trattamento dei segnali, quindi di per sé non incide sulle preoccupazioni di cui l'onorevole era portatore.

Per quanto riguarda la domanda dell'onorevole Cassola, anch'essa molto puntuale, credo che la spiegazione sia molto banale - spero di non dire sciocchezze - e sia dovuta al fatto che il GPS nasce in ambito militare.

È chiaro che l'integrazione fra GPS e Galileo deve scontare il fatto che i due sistemi si differenziano, anche da questo punto di vista. Come ho detto, infatti, il GPS nasce e continua a essere un sistema geosatellitare di origine militare, che peraltro stiamo utilizzando tutti.

Del resto, Galileo non esiste ancora. Quindi, quando usiamo i nostri sistemi di localizzazione, tendenzialmente ci serviamo del GPS che nasce e rimane, innanzitutto, indirizzato a finalità militari.

Già questa può essere una spiegazione ragionevole della differenza esistente. Negli altri casi, invece, si tratta di dialogare con delle nazioni, più che con sistemi già operativi. Pertanto, nel caso di Israele, ad esempio, si può decidere di integrare la sua partecipazione a Galileo, ma essenzialmente a fini civili. Non so se mi sono spiegato.

ARNOLD CASSOLA. Proprio perché è nato nel campo militare, non è ancora più importante specificare l'utilizzo civile?

PRESIDENTE. Articolo 4, comma 3...

FRANCESCO PIZZETTI, *Presidente dell'Autorità garante per la protezione dei dati personali*. Ho dato una risposta specifica del motivo della differenza. Il resto riguarda una valutazione di tipo obiettivamente politico. Naturalmente, va tenuto a mente il sistema di alleanze, anche militari, in cui gli stessi Paesi dell'Unione europea sono inseriti.

Ovviamente, questo aspetto non riguarda il Garante, il quale può solo ricordare che anche Galileo potrebbe essere utilizzato per finalità di sicurezza, di giustizia e di difesa. Quindi, anche noi lo costruiamo come un sistema neutro, perché fatto di ripetitori, ma potenzialmente predisposto anche per quel tipo di finalità. La domanda era puntuale e la risposta era giustificato che fosse puntuale.

L'onorevole Picano mi ha rivolto una serie di domande che ci spostano su un'altra tematica, comunque di assoluta e permanente attualità, ossia quella delle intercettazioni telefoniche.

Credo che in proposito il Garante non abbia granché da rimproverarsi, perché la nostra valutazione è stata espressa molte volte. Quello che abbiamo potuto fare è cercare di mettere in sicurezza il rapporto fra gestori telefonici e autorità giudiziaria,

affinché non ci siano fughe illecite di notizie. Anticipo che continueremo a lavorare sugli uffici giudiziari.

Quanto prima, credo questa settimana, sarà reso noto il nostro provvedimento sul Tribunale di Roma, al fine di spingere gli uffici giudiziari a tutelare i dati in loro possesso anche, e prima di tutto, nell'interesse della giustizia.

Ovviamente, i dati personali di cui l'ufficio giudiziario è in possesso sono una quantità enorme. Molte volte sono più preziosi quelli in possesso del giudice civile, che quelli in possesso del giudice penale. Pensate, ad esempio, ai dati di una controversia ereditaria o di un'interdizione per malattia mentale, o di una separazione fra coniugi che devono discutere della ripartizione patrimoniale e dell'affidamento dei figli. Quindi, è importante che la protezione dati riguardi anche i giudici e gli uffici giudiziari.

Sulle intercettazioni telefoniche, il Garante ha adottato provvedimenti nell'ambito della competenza istituzionale attribuitagli. Il resto è un problema di codice di procedura penale, da un lato, e di codice deontologico dei giornalisti, dall'altro.

Il principio di libertà di informazione, quindi di utilizzabilità, a fini di cronaca, delle notizie lecitamente acquisite dai giornalisti, è un cardine fondamentale del nostro sistema democratico. Tuttavia, il codice deontologico detta ai giornalisti le regole per un corretto uso del loro dovere di informare (che non è neanche libertà di informare, perché la libertà è quella dei cittadini di essere informati).

A questo molte volte ci appelliamo, qualche volta interveniamo, non sempre con un'adeguata comprensione da parte dell'opinione pubblica. D'altra parte, anche questo è giusto, perché il dibattito pubblico è essenziale anche per controllare il Garante. In alcuni casi, abbiamo dato valutazioni che l'opinione pubblica ha variamente giudicato.

Il problema grosso riguarda il codice di procedura penale. Questo lo sapete, vi è noto. Avete in discussione il disegno di legge Mastella sulle intercettazioni telefo-

niche, ma vi era già un disegno di legge Flick due legislature fa, teso a stabilire quale sia il confine della tutela del segreto istruttorio e quale quello delle notizie pubblicabili. Un ulteriore punto importante era quello relativo a come mettere a sistema tre diritti fondamentali: il diritto-dovere del giudice a esercitare l'azione penale, il diritto dell'imputato a difendersi - per cui l'interessato deve avere, ovviamente, le informazioni necessarie per difendersi, altrimenti ci troviamo in un processo inquisitorio di altre epoche storiche - e il diritto a informare, fondamentale per un corretto funzionamento della società democratica.

All'interno di questi valori, tutti e tre fondamentali, si trova la problematica che solo il Parlamento può sciogliere.

Il Garante ha fornito spesso delle indicazioni e si è esposto a volte anche in modo non del tutto condiviso. Tuttavia, per quanto ci riguarda, oltre un certo limite non possiamo andare.

Quanto alle chiamate telefoniche non richieste, onorevole Picano, non c'è dubbio che tale problema sia enorme.

Da sei mesi, stiamo lavorando con i gestori telefonici, per invitarli a rispettare le regole previste dalla normativa in materia di protezione dei dati personali, almeno quando i loro *call center* sono utilizzati dai gestori telefonici stessi. Abbiamo adottato provvedimenti, abbiamo anche chiesto onerosi investimenti da parte dei gestori per limitare questo cattivo uso dei dati personali. Non ci sfugge che il problema persista.

Dico con franchezza - e sempre nella consapevolezza assoluta della sede in cui opero - che siamo di fronte a un dilemma, che è bene condividere con il Parlamento. Abbiamo il potere e lo strumento per stroncare questo fenomeno. Questo, però, significa chiudere i *call center* e adottare provvedimenti che vietino l'uso di queste strutture. Infatti, il *call center* che operi in termini di violazione della normativa sulla *privacy* può essere oggetto di un provvedimento di blocco e di divieto del trattamento dei dati, che può anche portare alla sua chiusura.

D'altra parte, come sapete, questi centri danno occupazione a un numero molto elevato di giovani, spesso in condizioni precarie di lavoro. Inoltre, operano - non per colpa dei ragazzi che vi lavorano, ma per le modalità di organizzazione che li regolano - in modo legittimo e, contemporaneamente, illegittimo.

Vale a dire che se chiamano a casa, per fornire un'informazione richiesta, offrono un servizio. Una persona, ad esempio, può aver chiesto, anche al proprio gestore telefonico, di essere informata circa le nuove opportunità di risparmiare sul costo dell'abbonamento telefonico.

Se invece chiamano in assenza di una richiesta da parte del ricevente, violano la sfera di libertà personale, compiono un'azione illegittima.

Spesso ci siamo interrogati circa il nostro « rimanere in mezzo », divisi tra la domanda sociale di intervento che ci viene posta e la preoccupazione che abbiamo di non operare un intervento che possa essere eccessivamente devastante rispetto a un settore molto specifico, ma altrettanto importante, dell'attività economica e lavorativa in atto.

Lo ripeto, sono state numerose le occasioni in cui siamo stati sul punto di procedere all'attuazione di provvedimenti di blocco. Credo che se il fenomeno continuasse dovremmo operare in questo senso. Speriamo che, ove questo avvenisse, l'opinione pubblica ci capisca e non rimanga preda delle dichiarazioni che sicuramente circoleranno, ossia che il provvedimento del Garante mette sul lastrico centinaia di migliaia di giovani. A quel punto, infatti, i *call center* non potrebbero

più mantenere la loro attività. Quindi, con un fondamentalismo eccessivo, avremmo determinato un grave danno all'economia italiana.

Del resto, ci capita frequentemente di trovarci nella difficoltà di spiegare le nostre ragioni, pur essendo sempre molto consapevoli della complessità sistemica dei problemi in gioco.

Non ricordo se vi sono altre questioni puntualmente richieste da soddisfare. Mi sembra, tuttavia, di aver risposto almeno alle domande essenziali.

Il clima complessivo dell'audizione, almeno da parte mia e dei colleghi presenti, ci spinge a ringraziarvi sentitamente del tempo che ci avete dedicato, perché questa è stata anche una bella occasione per condividere con il Parlamento i nostri problemi.

PRESIDENTE. Come avevo già preannunciato, penso che avremo ulteriori occasioni per dialogare in maniera anche puntuale, rispetto ad alcuni provvedimenti.

Nel ringraziare il presidente Pizzetti per la disponibilità manifestata, dichiaro conclusa l'audizione.

La seduta termina alle 11,50.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. COSTANTINO RIZZUTO

Licenziato per la stampa
il 15 gennaio 2008.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

