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 compartecipare 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 anche 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 delicata, 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, semplicemente 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 salvare 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 quesiti 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 cervellone 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 cervellone 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 chiedevo 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 soggetto, 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 –