COMITATO PARLAMENTARE DI CONTROLLO SULL'ATTUAZIONE DELL'ACCORDO DI SCHENGEN, DI VIGILANZA SULL'ATTIVITÀ DI EUROPOL, DI CONTROLLO E VIGILANZA IN MATERIA DI IMMIGRAZIONE

RESOCONTO STENOGRAFICO

AUDIZIONE

12.

SEDUTA DI MARTEDÌ 3 MARZO 2015

PRESIDENZA DELLA PRESIDENTE **LAURA RAVETTO**

INDICE

PAGINA BIANCA

PRESIDENZA DELLA PRESIDENTE LAURA RAVETTO

La seduta comincia alle 9.05.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata attraverso la trasmissione diretta sulla *web-Tv* della Camera dei deputati.

(Così rimane stabilito).

Audizione del Garante per la protezione dei dati personali, on. Antonello Soro.

PRESIDENTE. L'ordine del giorno reca l'audizione del Garante per la protezione dei dati personali, onorevole Antonello Soro, nelle materie di competenza del Comitato, con particolare riferimento alle problematiche connesse alla protezione dei dati personali, in relazione al fenomeno dell'immigrazione.

Il presidente Soro è accompagnato dalla dottoressa Federica Resta, assistente giuridica del presidente, e dal dottor Mario De Bernart, dirigente del servizio relazioni istituzionali.

Ringraziamo il presidente della presenza. Presidente, noi l'abbiamo invitata perché il Comitato ha avviato un'indagine conoscitiva generale sui flussi migratori, nel corso della quale, dopo aver trattato i temi di competenza strettamente nazionale, ovvero l'analisi di Mare nostrum, il passaggio a Triton e la situazione dei minori che arrivavano nel nostro Paese, ha dovuto anche affrontare alcuni elementi relativi più propriamente alla potenzialità delle infiltrazioni terroristiche.

Abbiamo ascoltato gli *opinion leader* su queste tematiche. Abbiamo ascoltato il sottosegretario Minniti, giovedì abbiamo il Ministro Gentiloni. Abbiamo ascoltato più volte il Ministro Alfano. Abbiamo ascoltato il capo della polizia Pansa la scorsa settimana. Tutti, da una parte, ci hanno molto tranquillizzato sull'assenza di potenziali infiltrati nell'ambito degli sbarchi sulle nostre coste. Tuttavia, dall'altra parte, ci hanno dato sia degli elementi di riflessione sul fatto che probabilmente almeno organizzazioni criminali, se non propriamente terroristiche, potrebbero entrare o sarebbero già nell'attività di gestione di questi migranti sia degli elementi più propriamente di pericolosità generale sul nostro territorio.

In particolare, sono sempre stati trattati i temi del flusso di dati, da una parte come la possibilità di individuare sia i soggetti che arrivano nel nostro Paese sia i soggetti che potrebbero essere organizzatori di questi passaggi, dall'altra in relazione ai fatti che sono accorsi recentemente in Francia.

Effettivamente abbiamo rilevato delle situazioni che ci hanno lasciati perplessi, una su tutte quella della fidanzata di uno degli attentatori, compartecipe agli atti terroristici, che con molta tranquillità è partita da un aeroporto internazionale, senza che nessuno avesse un *data record* tale da poterla fermare, quando c'era tutta la polizia francese che la stava cercando.

A questo punto, abbiamo ascoltato tutte le personalità interessate al trattamento dei dati, per capire come sia possibile che a livello europeo non ci sia uno scambio o comunque non ci sia una sorta

di *database* globale, con tutti i dati dei soggetti, come succede invece negli Stati Uniti.

Abbiamo raccolto opinioni talvolta anche difformi, però su un punto tutti sono stati abbastanza unanimi. Da una parte, tutti ci hanno detto che sarebbe utile avere quello che viene chiamato PNR *(Passenger name record)*, una raccolta a livello europeo di dati tale da consentire alle autorità di controllo, di vigilanza e di polizia di poter accedere ai dati dei soggetti che entrano o escono dallo spazio Schengen. Dall'altra, ci hanno fatto notare come sia difficile in pratica, addirittura per Europol, avere questi dati.

È venuto qua il direttore generale di Europol, il quale ci ha detto: « Io a volte ho difficoltà con i ministri degli interni dei vari Stati, perché ogni Stato ha una propria disciplina della *privacy* e ogni Stato muove delle corrette osservazioni ».

Siamo qua a chiederle un parere in merito. Abbiamo visto le sue dichiarazioni. Abbiamo visto in particolare la sua osservazione. È stato l'unico che l'ha fatta. Naturalmente questa sua dichiarazione ci ha fatto riflettere. Lei – ci corregga se sbagliamo – ha detto: « Benissimo i *database*, però attenzione, perché, oltre ai limiti della *privacy*, queste potrebbero addirittura trasformarsi in piattaforme che facilitano l'accesso ai gruppi terroristici e che possono essere *hackerate*, come si dice in gergo ».

Abbiamo letto quello che è successo ieri, se veramente è successo. Aspetteremo di avere delle precisazioni. Mi riferisco alla scuola a San Severino Marche, la cui struttura informatica pare essere stata *hackerata*.

Chiaramente la riflessione c'è e vogliamo delle sue considerazioni. In particolare, abbiamo letto su *Avvenire* del 12 febbraio 2015 una sua intervista, dove lei ha richiamato la necessità di un'efficace azione di prevenzione del terrorismo e la selezione di obiettivi sensibili in funzione del loro grado di rischio e auspicava che la protezione dei dati diventasse una condizione strutturale della *cyber security*. Su questo vorremmo dei primi commenti.

Sempre con riferimento al rapporto tra protezione dei dati e *cyber* sicurezza, sappiamo che il Governo sta adottando uno schema di regolamento che istituirà la banca dati nazionale, che è prevista dal Trattato di Prüm del 2005, proprio per rafforzare la cooperazione transfrontaliera nel contrasto al terrorismo. Anche su questo le chiediamo un commento.

Le ho accennato al PNR. Le chiediamo se può darci delle indicazioni. Sappiamo che ci furono molti tentativi a livello europeo. Sappiamo cosa ne ha detto lei, ma anche i garanti della *privacy* dei vari Stati. Lo stesso garante francese, subito dopo gli accadimenti di Charlie Hebdo, comunque si è espresso nel senso della cautela.

Più in generale, vorremmo il suo parere sull'armonizzazione delle regole sulla *privacy*. Ci aiuti a capire che cosa si può migliorare. Il Comitato può anche dare dei suggerimenti, quando abbiamo la possibilità di avere audizioni.

Il capo della polizia, il prefetto Pansa, nella sua recente audizione, come le dicevo, ha segnalato che non soltanto Europol incontra delle difficoltà nell'utilizzo dei dati sensibili, ma anche Frontex, anche perché c'è una differenza nella disciplina della *privacy* dei vari Paesi europei.

Naturalmente, dopo la sua relazione, i colleghi avranno la possibilità di porle delle domande. Se vorrà rispondere in sede di Comitato, le saremmo grati. Altrimenti, può tornare in replica.

Cedo la parola a Antonello Soro, Garante per la protezione dei dati personali, per lo svolgimento della sua relazione.

ANTONELLO SORO, *Garante per la protezione dei dati personali*. Ringrazio il presidente e il Comitato per offrire questa occasione di comunicarvi un punto di vista che, rispetto a quelli numerosi e importanti già auditi nelle settimane scorse, potrebbe essere, non tanto diverso, quanto frutto di una peculiare funzione dell'autorità che io rappresento, che ha come missione la tutela di un interesse eminen-

temente individuale: il diritto fondamentale di ciascuno di noi alla protezione dei dati personali.

Voglio dire subito che da questo punto di vista alcune delle premesse fatte dal presidente mi sollecitano due considerazioni di fondo.

In primo luogo, non è fondata l'idea che in Europa esistano ordinamenti in materia di tutela dei dati personali così difformi. Esiste una direttiva ed esiste un progressivo affinamento e armonizzazione dei comportamenti delle singole 28 autorità nazionali, che hanno un organo di coordinamento che si riunisce con periodicità costante.

Esistono sicuramente – poi ne parlerò – dei livelli di capacità e di efficienza del sistema di attuazione della direttiva che possono essere diversi, ma tendenzialmente la cornice giuridica è una cornice europea, così come è una cornice ineludibile nella discussione che oggi noi stiamo facendo il livello nuovo della giurisprudenza europea. Ci sono state, infatti, sentenze molto rilevanti.

Tra queste, richiamerò nel corso delle mie comunicazioni la cosiddetta « sentenza *Data retention* », quella che ha stabilito la non coerenza con l'ordinamento europeo di una direttiva che è stata di fatto annullata, perché consentiva la conservazione indiscriminata per un tempo lungo, uguale per tutti, indipendentemente dai reati per i quali potessero essere accertati, dei dati di traffico.

Dunque, la cornice giuridica su cui noi dobbiamo muoverci è importante. Questa sentenza *Data retention* indica un percorso che è fondamentale anche nella fase molto delicata nella quale noi ci troviamo.

Il diritto alla protezione dei dati personali – spero di riuscire a spiegarlo – solo apparentemente è in antitesi con interessi collettivi quali la sicurezza pubblica, l'accertamento e la prevenzione dei reati, essendo invece legato a essi da una sinergia assai profonda.

Cercherò di rispondere alle sollecitazioni, partendo da una considerazione generale. La protezione dei dati personali è essa stessa essenziale presupposto, non solo della *cyber security,* ma più in generale della sicurezza pubblica nell'epoca di internet.

Aggiungo una brevissima considerazione generale. Nella società digitale nella quale siamo profondamente immersi, i dati personali non sono astrazioni, cifre, dati aridi che vengono immessi in un computer, ma sono la nostra vita che si svolge nella nuova dimensione che è la dimensione digitale, una dimensione uguale a quella dello spazio fisico nella quale, invece, si vive l'esperienza fisica di tutte le nostre persone.

Pertanto, la protezione dei dati che sono all'interno della dimensione digitale significa la protezione delle persone. Questa è la premessa essenziale al di fuori dalla quale si rischia di identificare la tutela della *privacy* con un profilo, assolutamente fondamentale anch'esso, di riservatezza. La dimensione della protezione dei dati nella società digitale acquista un'altra valenza, una valenza assoluta: la protezione dei dati è il primo diritto della società digitale.

Da questa considerazione muove la seconda: se le banche dati strategiche su cui si fonda l'intero sistema di sicurezza pubblica e quello della prevenzione non sono adeguatamente protette, non soltanto quei pezzi di vita archiviati e racchiusi negli archivi digitali, ma anche le nostre persone e, quindi, il sistema democratico diventano vulnerabili.

Nelle carenze delle misure di protezione dei dati e dei sistemi pubblici e privati si insinua, infatti, l'azione del crimine organizzato e del terrorismo, che sempre più si avvalgono del patrimonio informativo di cui dispongono soprattutto le amministrazioni pubbliche, ormai assurte, secondo gli analisti, a obiettivi preferenziali di attacchi cibernetici dimostrativi, quando non addirittura terroristici.

Ciò avviene soprattutto in ragione dell'asimmetria tra l'accrescimento del potere informativo nelle pubbliche amministrazioni e le strategie di sicurezza che hanno caratterizzato il processo di informatizzazione in Europa e particolarmente in Italia, perché di questo ci stiamo occupando.

Il sistema di digitalizzazione della pubblica amministrazione, dopo una disordinata, sporadica e in qualche misura contraddittoria fase di avvio nelle amministrazioni locali e in quella centrale, oggi viaggia abbastanza velocemente, in una fase di oggettiva asimmetria rispetto, invece, alla protezione dei dati personali e alla sicurezza informatica di questi grandi raccoglitori di informazioni.

Recentemente l'Università La Sapienza di Roma ha presentato una ricerca sullo stato di sicurezza della pubblica amministrazione italiana a livello centrale, regionale e comunale, dimostrando, sulla base di questa ricerca, che i livelli di protezione e di vulnerabilità delle amministrazioni pubbliche nella scala nazionale, regionale e locale è disastrosa. Si passa da livelli di protezione reale efficiente del 18-19 per cento nei comuni a livelli del 25-30 per cento nelle regioni, per arrivare poco sopra il 50 per cento nell'amministrazione centrale.

Pertanto, la protezione delle banche dati è un tema su cui noi abbiamo il compito di richiamare l'attenzione.

Proteggere i dati personali da un 11 settembre digitale è il primo presupposto per la sicurezza individuale e collettiva, che necessita, dunque, non solo di accorgimenti adeguati, ma anche di una complessiva razionalizzazione del nostro sistema informativo.

Il tema – lo richiamava la presidente poc'anzi – diventa quello di ridurre la superficie di attacco. Sia il terrorismo che la criminalità organizzata rappresentano una grandissima minaccia. La minaccia cibernetica non investe soltanto terrorismo e criminalità organizzata, ma investe la nuova dimensione del conflitto internazionale. Se è vero che la superficie d'attacco è ridotta, quella è una strategia difensiva di per sé importante.

Pertanto, l'idea di limitare la raccolta di informazioni a quelle davvero necessarie diventa una strategia di politica di difesa degli Stati, delle infrastrutture comuni e della sicurezza dei cittadini.

Ridurre la superficie d'attacco, evitando raccolte massive di dati, che finiscono con l'essere inutili, perché ingestibili, è in questo senso una condizione indispensabile per la sicurezza pubblica, che va garantita con il ricorso a strumenti investigativi capaci di selezionare adeguatamente gli obiettivi sensibili e non certo con la pesca a strascico nelle vite degli altri, come ha ribadito la Corte di giustizia nella sentenza che richiamavo.

Vorrei ricordare una condizione vissuta dal mondo soltanto due anni fa. Le rivelazioni di Snowden hanno messo in evidenza non solo il rischio per la vita privata dei cittadini, ma anche l'inutilità di un sistema di raccolta massivo, che ha preteso di immagazzinare tutti i dati di traffico, tutte le informazioni e tutta la comunicazione che transitava per i telefoni e per la via informatica.

Questa si è rivelata, per riconoscimento non soltanto europeo, ma degli stessi Stati Uniti, una strada sbagliata.

Noi siamo passati in queste settimane da una profonda emozione legata al *Datagate* e, quindi, all'attenzione nei confronti della *privacy* a un'altrettanta radicale preoccupazione per la sicurezza. Si è cominciato a dire: « Il problema non è la *privacy*, ma è la sicurezza ».

In realtà, sono due facce di una stessa medaglia e dobbiamo avere l'intelligenza di muoverci in questa dimensione non sulla base di una spinta emotiva, naturalmente mutevole e spesso, come in questo caso, contraddittoria, ma sulla base di una conoscenza reale e di uno sforzo reale nel trovare il punto di equilibrio nuovo che in queste circostanze va sempre ricercato.

Il valore aggiunto della protezione dei dati per l'azione antiterrorismo consiste nella valorizzazione della natura mirata e selettiva delle indagini, nell'esigenza di accrescere la capacità difensiva dei nostri sistemi, rappresentandone un fattore abilitante.

Questa è la cifra che noi abbiamo cercato di imprimere all'azione del Garante in questi anni, nell'attività di complessiva messa in sicurezza dei centri privati e pubblici di raccolta dei dati

personali e delle stesse infrastrutture dirette su cui viaggiano i flussi informativi fra le amministrazioni.

Mi riferisco, ad esempio, all'attività svolta rispetto a banche dati strategiche per la sicurezza pubblica, quali quelle incardinate presso il Dipartimento di polizia del Ministero dell'interno e la costituenda Banca dati nazionale del DNA al CED interforze.

Sotto questo profilo, rilevantissimi sono i sistemi informativi funzionali agli adempimenti previsti dall'accordo di Schengen e dalla Convenzione di Dublino, quale la Banca dati nazionale dei permessi di soggiorno, comprensiva dei dati di tutti i migranti presenti sul territorio, che si affianca al flusso informativo diretto a Eurodac, relativo ai dati, anche biometrici, di richiedenti asilo e stranieri fermati alla frontiera o irregolari.

Particolarmente importante è poi la sezione nazionale del sistema informativo Schengen, il cosiddetto NSIS *(National Schengen information system*), rispetto al quale il Garante è designato autorità di controllo incaricata di verificare la correttezza del trattamento effettuato, attività che ha portato a una serie di provvedimenti prescrittivi volti a rafforzare il livello di sicurezza di questi sistemi.

Allo stesso modo, devono essere considerati non come scomodi adempimenti, ma come contributi al miglioramento della sicurezza complessiva dei sistemi e, quindi, della sicurezza pubblica i controlli sul rispetto della disciplina della *privacy* da parte di agenzie come Europol.

Attraverso l'innalzamento del livello di protezione dei dati e dei sistemi di cui Europol si avvale, infatti, si realizza un complessivo miglioramento della capacità difensiva dell'Unione rispetto al rischio di attacchi terroristici o comunque all'azione del crimine organizzato.

In questa sede ho avuto modo di leggere le dichiarazioni del vicedirettore di Europol, Orlandi, che avrebbe osservato che il sistema Schengen è solo a livello *basic* e, quindi, potrebbe essere facilmente intercettato.

Dice Orlandi: « Se pensate che gli avversari potenziali di questi sistemi sono Paesi e organizzazioni che possono avere a libro paga matematici russi, esperti di crittografia » – non so perché abbia considerato i russi più bravi, visto che ce ne sono di bravi anche altrove – « vi rendete conto come avere una rete a livello di riservatezza e di segretezza sia senz'altro un *asset* interessante ».

Citerei per analogia un *data breach* del sistema SIRENE danese, che si è verificato nel 2013, che dimostra come questi sistemi sono vulnerabili.

Resta comunque il rischio generale di ogni sistema informatico, anche se a livello europeo c'è oggi una nuova attenzione ed è stata creata un'agenzia, Eu-LISA, proprio per la sicurezza dei sistemi informatici SIS, VIS *(Visa information system*) e Eurodac.

Questo aspetto dovrà essere tenuto ancora di più in considerazione con il nuovo regolamento sull'Europol, che configura tale ente come piattaforma di interscambio di informazioni essenziale per la cooperazione di polizia e giudiziaria, mediante il collegamento a Eurojust, tra gli Stati membri, con un accrescimento del potere informativo che deve essere, a nostro parere, accompagnato da adeguate garanzie.

Del resto, in un contesto in cui già oggi nel SIS *(Schengen information system*) vi sono più di 880.000 nominativi di persone, della maggior parte delle quali si vieta l'ingresso nell'Unione, è evidente come il problema non sia tanto l'ostacolo all'acquisizione dei dati, quanto la loro efficace analisi e gestione, quindi il fattore umano, che diventa decisivo nell'uso delle informazioni che vengono raccolte, vincendo la tentazione, che è una tentazione culturale del nostro tempo, di delegare alla tecnologia funzioni che sono propriamente dell'intelligenza dell'uomo.

Nella logica di contribuire a elevare i livelli di sicurezza dei sistemi e con essi dei dati ivi contenuti, il Garante ha siglato con il Dipartimento di informazione e sicurezza un protocollo d'intenti – so che ne ha fatto cenno in questa sede il sotto-

segretario Minniti – per disciplinare alcune procedure informative specifiche e innovative, perché di carattere sistematico, relative alle garanzie osservate dai servizi nei trattamenti dei dati personali da loro svolti, soprattutto a seguito dell'attribuzione all'agenzia della specifica competenza sulla *cyber security*.

Tale forma di esercizio dei poteri dell'Autorità è maggiormente corrispondente alle peculiarità che caratterizzano oggi le attività delle agenzie e ai loro poteri di accesso sistematico, che, se non adeguatamente esercitati con l'indispensabile fattore umano, possono davvero degenerare in una forma di sorveglianza totale, dannosa per i cittadini e non utile alla sicurezza pubblica.

Il nostro rapporto con gli organismi di sicurezza è il primo caso in Europa di disciplina di procedura informativa a carattere strutturato tra autorità di protezione dei dati e organi tradizionalmente sottratti ai controlli esterni, come sono quelli dell'*intelligence*.

In questa direzione dovrebbe condurre il passaggio sull'esigenza di un pieno controllo giudiziario e democratico delle politiche antiterrorismo e dell'attività di *intelligence*, contenuto nella recentissima risoluzione del Parlamento europeo votata l'11 febbraio scorso.

Vengo infine al tema PNR. Un equo bilanciamento tra *privacy* e sicurezza può stabilirsi anche rispetto alla disciplina del PNR, ovvero della cessione da parte delle compagnie aeree alle autorità inquirenti delle informazioni riguardanti i passeggeri e le relative prenotazioni.

Il testo originario della direttiva – lo ricordava la presidente – non aveva trovato nel 2011 condivisione nel Parlamento europeo e nel *Working Party 29*, che è l'organo di raccordo delle autorità di protezione dati dei vari Stati membri, i quali avevano invitato la Commissione a valutare alternative meno invasive.

Pertanto, soprattutto dopo il test di proporzionalità imposto agli strumenti investigativi dopo la sentenza *Digital rights*, va oggi attentamente valutata la possibilità di ricorrere a mezzi alternativi altrettanto efficaci, aspetto sul quale, tuttavia, si registrano posizioni diverse e non necessariamente inconciliabili.

A fronte di chi avanza dubbi sulla reale utilità investigativa di questi dati, altri, invece, sottolineano come soltanto il PNR coniugherebbe funzione reattiva per l'accertamento di un reato connesso a funzione proattiva e preventiva, tale cioè da impedire delitti futuri.

Solo i dati PNR potrebbero, infatti, individuare soggetti non noti da sottoporre a ulteriore verifica, a differenza dei dati API *(Advance passenger information*) o raccolti mediante i sistemi SIS e VIS (informativo di Schengen e informazione visti), che riguardano persone attinte da già precedenti segnalazioni o comunque informazioni utili alla gestione delle frontiere.

In ogni caso, anche qualora il test di proporzionalità venisse superato, la direttiva PNR, a nostro parere, dovrebbe assicurare alcune modifiche essenziali rispetto al testo originario del 2011.

In particolare, dovrebbe restringere il novero dei procedimenti nell'ambito dei quali acquisire tali dati a quelli per terrorismo e criminalità organizzata transnazionale, superando le più ampie categorie di *serious crime* e di delitti per i quali è emesso il mandato d'arresto europeo.

Inoltre, dovrebbe ridurre il termine di conservazione dei dati. Secondo il relatore attuale, il termine di conservazione sarebbe di 30 giorni in chiaro, più cinque anni per terrorismo e quattro per i seri crimini transnazionali, in questo caso con dati mascherati, con un'articolazione della conservazione sulla base della specifica, abbastanza in coerenza con le indicazioni della sentenza *Digital rights*.

La direttiva dovrebbe poi subordinare il trasferimento dei dati a Paesi terzi all'autorizzazione dell'autorità giudiziaria o dell'autorità di protezione dati.

Dovrebbe, altresì, limitare le informazioni ai soli voli extra UE. Su questo tema esiste una posizione molto controversa. Il relatore stesso, che è un inglese, propone di estenderle anche ai voli interni all'Unione europea.

Dovrebbe, infine, prevedere il ricorso esclusivo al metodo *push* e non *pull*, impedendo agli Stati l'accesso diretto ai *database* delle compagnie, ferme restando le previsioni contenute nel testo già dal 2011 sui diritti dell'interessato e sul divieto di profilazione sulla base dei dati sensibili.

In favore della direttiva depone oggettivamente l'esigenza di armonizzare le varie normative nel frattempo introdotte autonomamente dai vari Stati membri, superandone le difformità, che non solo ostacolano la cooperazione di polizia giudiziaria in questa materia – oggettivamente non brillante, come mi pare di cogliere anche dalle precedenti audizioni da voi effettuate – ma rischiano di determinare disparità di trattamento nell'esercizio di un diritto fondamentale quale quello alla protezione dei dati.

Con il nuovo quadro giuridico europeo attualmente in discussione – si conta di avere l'approvazione del pacchetto di riforma in materia di protezione dei dati entro il 2015 o al massimo nella prima parte del 2016 – di fronte a questa ipotesi e a quella più anacronistica della chiusura dello spazio Schengen, dovremmo ricordare che un'adeguata legislazione sulla protezione dei dati è sempre stata la condizione posta ai vari Governi, il nostro per primo, per farvi parte.

In Italia si è fatta la prima legge in materia di protezione dei dati personali sotto la spada di una non ammissione allo spazio Schengen. Paradossalmente, oggi dovremmo riconsiderare la presenza di una seria protezione dei dati personali come il modo più efficace – lo era già in origine – per difendere la dimensione, la cultura e la filosofia dello spazio Schengen, a dimostrazione di questa sinergia tra protezione dati e sicurezza, in un mondo che per fortuna ha visto cadere più di una barriera.

Io mi fermo qui, presidente. Mi scuso se sono stato disordinato.

PRESIDENTE. Grazie, presidente. Si conferma che lei mantiene questo *status* di avanguardia in Italia. Sono certa che le sue osservazioni verranno tenute in debita considerazione anche a livello europeo.

Noi naturalmente ci faremo portavoce di queste sue istanze. Anche qui si è discusso sui voli extra UE e intra UE e, quindi, le sue osservazioni saranno per noi motivo di approfondimento in questo senso, anzi ci riserviamo di richiamarla in futuro, quando vedremo che la materia viene sviluppata in maniera dettagliata.

Do la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

RICCARDO CONTI. Conoscendo il nostro ospite e interlocutore, immaginavo che facesse una relazione solida. Questo mi consente, anziché di fare tanti ragionamenti, di restringere il mio intervento a una domanda.

Io ho una collaboratrice familiare, che è una colf regolarmente assunta qui a Roma, che è molto intelligente e mi fa sempre delle domande prima che io esca di casa o quando arrivo.

Questa signora dice: « Vi rendete conto voi che tutte le vostre banche dati delle organizzazioni pubbliche ai vari livelli, periferiche e centrali, forse contengono meno dati di quelli che possiedono alcune *lobby* del commercio, dell'industria e del credito ? ».

La nostra vita è vivisezionata in tutti gli aspetti. Sempre secondo questa signora, tutti questi dati vengono venduti e rivenduti da tutte le parti, senza che nessuno abbia la possibilità di interferire in questa cessione di dati. Quello che appare è un conto e quello che poi fanno nella cessione di questi dati è un altro.

La domanda che vorrei rivolgerle è questa: chi è l'autorità che concretamente vigila sui passaggi di dati tra i vari raccoglitori di dati ? La mia domanda è proprio tecnica, nel senso che io vorrei sapere chi vigila concretamente, non politicamente, cioè chi – un Parlamento, un Governo o qualsiasi istituzione – è in grado tecnicamente di garantire che non ci siano deviazioni nell'utilizzo dei dati da chiunque raccolti, dal pubblico o dal privato, per le varie necessità.

ANTONELLO SORO, *Garante per la protezione dei dati personali*. Ringrazio molto il senatore Conti, perché pone un tema che supera lo specifico o lo comprende in qualche modo: la dimensione globale della società digitale.

I nostri dati, che vengono raccolti da uno *smartphone*, vengono canalizzati attraverso un percorso molto lungo e normalmente vanno a essere poi contenuti in un server che si trova in una qualche parte del mondo. Non sempre questo server è in una posizione nota.

La generazione del *cloud computing* ha di fatto trasformato anche la capacità di controllo dei dati da parte del cittadino, un controllo che è il fondamento della direttiva europea in materia di protezione dati, rendendo arduo il compito di coloro che hanno la competenza specifica di vigilare.

Aggiungo che questo percorso è regolato da una filosofia primaria, che è quella della profilazione. Le grandi imprese digitali nel mondo sono un oligopolio nella raccolta dei dati, finalizzati a definire profili che devono a loro volta essere utilizzati come la merce più ricca e più importante nel rapporto fra produttori e consumatori nell'economia globale.

Abbiamo un dato che ha trasformato in pochissimi anni l'economia globale, attribuendo a queste società una ricchezza spropositata e un potere non solo economico, ma anche politico di interferenza sui Governi (trattano con gli Stati da pari a pari).

Abbiamo una società che improvvisamente ha trasformato una visione idilliaca della rete come lo spazio più grande di libertà in uno spazio nel quale esiste molta libertà, ma esistono anche dei padroni di cui abbiamo difficoltà a contenere l'azione.

Sappiamo, tuttavia, che questa azione è irrinunciabile nell'organizzazione della vita attuale, per cui sarebbero del tutto fuori posto una vocazione neoluddista o un intento tecnofobico, per abolire la società digitale. Siamo nella società digitale e dobbiamo farci carico di governarla.

Come si può governare questo processo ? Naturalmente è un'impresa difficile, che richiede un'enorme cooperazione internazionale.

Nella dimensione europea, noi abbiamo uno standard di protezione dati più alto rispetto alla generalità degli altri spazi del mondo, anche se molte parti del mondo vanno allineandosi agli standard europei.

Tuttavia, gli standard europei sono probabilmente insufficienti rispetto alla complessità della tecnologia che in questo periodo ha cambiato lo scenario. Gli strumenti che la direttiva europea e lo stesso regolamento che abbiamo in cantiere hanno identificato probabilmente non bastano, nel senso che sono fondati su alcuni presupposti e alcune fattispecie che sono propri di una società predigitale, quali il consenso e l'informativa.

Questi ultimi mantengono tutto il loro valore. Tuttavia, utilizzare l'arma dell'obbligo all'informativa e al consenso libero e consapevole per contenere l'irruzione nella vita e il potere di controllo, di sorveglianza e di orientamento che hanno le multinazionali digitali è un po' poco.

La conferenza mondiale dei garanti che si è svolta nell'ottobre scorso ha posto una serie di indicazioni.

Noi nella nostra dimensione – do conto di questo, perché forse vi è utile – abbiamo attivato un rapporto molto duro anche nei confronti di Google, non perché Google sia peggiore – probabilmente è quello più attento – ma perché è il motore di ricerca più potente in Europa. Infatti, il 90 per cento delle attività di raccolta dei motori di ricerca in Europa avviene attraverso Google, molto più di quanto avvenga negli Stati Uniti. Inoltre, Google ormai è una *holding* che ha 72 funzioni attive, che vanno dalla raccolta dei video fino alla posta elettronica e a tutto quello che può accadere nello spazio digitale.

Noi ci siamo proposti pretendendo da Google il rispetto delle norme dell'ordinamento europeo. Voi sapete che fino alla sentenza Google/Spain di un anno fa a qualunque osservazione da parte delle autorità europee Google rispondeva: « Voi non avete giurisdizione su di noi, perché la

nostra sede legale è negli Stati Uniti, quindi voi non potete chiederci niente ». Poi, sul piano di un *bon ton,* spesso hanno raccolto le nostre sollecitazioni.

Ora abbiamo fatto un passo decisamente più forte, nel senso che abbiamo fatto un provvedimento prescrittivo a Google, che si è impegnato a rispettarlo. Abbiamo anche sottoscritto un protocollo, che consente a noi di fare delle verifiche.

Io sono consapevole che tutto questo, se fatto da un singolo Paese, va nella giusta direzione. I colleghi delle altre autorità europee lo hanno condiviso. Infatti, insieme abbiamo poi votato un indirizzo in questa direzione, quindi credo che tutti insieme adesso faremo anche delle misure di *enforcement*, perché misurarsi con una potenza di queste dimensioni è assolutamente sbilanciato.

Detto questo, la strada per confermare questa complessità passa per una cultura della protezione dei dati che prima di tutto appartiene ai singoli. Ipotizziamo che noi utilizziamo lo spazio digitale per buttar dentro tutto quello che ci pare, al di fuori di qualunque ragionevolezza.

Io faccio sempre l'esempio della ragazzina che non si sognerebbe mai di mettersi nuda in terrazza o alla finestra, ma lo fa mettendosi dentro lo spazio digitale. Dobbiamo fare un enorme sforzo per recuperare la dimensione digitale, sapendo che non c'è nulla di segreto e che tutto quello che noi mettiamo lì dentro è violabile e in qualche modo oggetto di controllo.

Tuttavia, una cosa è violare la vita privata di un bambino, che è terribile, e un'altra cosa è rendere, per nostra incuria, violabile il patrimonio di informazioni strategiche di un Paese che si trova dentro le grandi banche dati che noi abbiamo costruito, che sono selettive e mirate, hanno un contenuto altissimo di riservatezza e vanno protette.

Colgo l'occasione per segnalare che, in questa dimensione di grande asimmetria fra l'oggetto del contrasto e il governo di questa complessità enorme, l'autorità che io presiedo è una piccola autorità.

Lo segnalo al Parlamento, perché mi capita spesso di incrociare qualcuno che mi dice: « Va bene, la *privacy*... ». La *privacy* è questo e rispetto a questo c'è un interesse strategico del Paese a creare risorse, prima di tutto umane e non economiche, sul fronte sul quale noi poi facciamo le ispezioni.

Concludendo, noi facciamo le ispezioni, andiamo nelle banche dati, verifichiamo che le compagnie telefoniche italiane siano in regola, abbiano rispettato le norme, abbiano secretato, abbiano criptato e abbiano fatto tutte le cose che noi abbiamo previsto.

Abbiamo prescritto alle procure della Repubblica di secretare seriamente le intercettazioni. È un percorso che non si è concluso. Mi auguro che si concluda rapidamente, perché tutti i dati delicati importanti della vita degli italiani, che per iniziativa della pubblica amministrazione vengono raccolti, devono essere anche protetti.

Questa è in fondo la filosofia che può valere forse più di un investimento economico, se entra nella dimensione della vita del Paese, della vita degli italiani e della vita di tutto il mondo. Infatti, noi siamo ormai un pezzo della vita di tutto il mondo.

GIORGIO BRANDOLIN. Io ringrazio il Garante per queste importanti informazioni che ci ha dato e anche per questo ultimo ragionamento, che mi ha stimolato nel fare alcune considerazioni.

In primo luogo, mi sembra che lei abbia detto che stiamo vivendo in questa era digitale, mentre ragioniamo ancora con degli strumenti – semplifico molto – che sono dell'era predigitale.

C'è difficoltà a correr dietro all'innovazione che avviene nel mondo della rete di mese in mese e di anno in anno. Non è un qualcosa di acquisito che si può affrontare avendo ben capito quali sono le sue capacità. Dunque, immagino la difficoltà di avere degli strumenti che passino dall'era predigitale all'attuale era digitale.

Mi viene una domanda rispetto a quanto ci ha detto prima. Anche se non rientra nei ragionamenti del nostro Comitato, a me ha colpito il fatto che la

sicurezza delle banche dati dei comuni è inferiore al 20 per cento, quella delle regioni al 30 per cento e quella dello Stato è vicina al 50 per cento.

Ovviamente ci riempiamo la bocca tutti, dicendo di volere digitalizzare tutto. Se queste sono le capacità delle nostre strutture dello Stato, delle regioni e dei comuni, sono un po' preoccupato.

Dico questo perché, giustamente, il Governo e il Parlamento stanno emanando direttive, decreti eccetera. Un po' tutte le categorie sono interessate da questo fenomeno.

Il sottoscritto, che fa il libero professionista, dal 30 marzo dovrà avere il collegamento e la possibilità di colloquiare con le strutture pubbliche solo in digitale. Personalmente, vedere che la protezione è inferiore al 20 per cento mi preoccupa un poco. Questa è una battuta.

Siete in grado di correre dietro alle innovazioni che il mondo della rete ha ? Di questo ovviamente siete consapevoli, perché l'avete detto. Vorrei sapere come lavorate, anche a livello europeo e sovranazionale, per avere degli strumenti che possano affrontare queste modifiche.

La seconda domanda che voglio porle è legata a un'osservazione che ha fatto poc'anzi. Noi viviamo in un mondo schizofrenico. Ha perfettamente ragione: fino a un anno fa con il Datagate eravamo tutti pro-*privacy,* adesso, da due mesi a questa parte, diciamo tutti che la *privacy* deve essere superata e l'importante è la sicurezza.

A proposito di questa consapevolezza che lei ha messo bene in evidenza, vorrei sapere quali sono le azioni che state facendo a livello europeo e quali sono i limiti fissi, oltre i quali non possiamo andare, per avere un po' più di garanzia dal punto di vista della sicurezza, mettendo insieme anche la *privacy*. Vorrei sapere se ci sono dei paletti che si possono definire oppure se anche questo è un argomento in essere, di giorno in giorno e di mese in mese.

PAOLO ARRIGONI. La presidente Ravetto aveva sottolineato la necessità di armonizzare le regole sulla *privacy*. Anche lei, presidente, ci è tornato.

Ovviamente questo fa presupporre che l'autorità che lei presiede sia in stretto contatto con le autorità o altri organismi simili dei Paesi europei e sicuramente con quelli facenti parte dell'area Schengen.

Vorrei sapere se voi avete rapporti o vorreste averne, per esempio, con i Paesi del Nord Africa o del Medioriente, che sono i Paesi di partenza di questo enorme flusso di immigrazione. Laddove questi mancassero, che cosa state facendo perché vengano attuati ?

La seconda domanda, invece, riguarda il fotosegnalamento. L'Italia è il Paese di primo approdo per i migranti che arrivano via mare e anche via terra. Spesso l'Europa ci ha strigliato, perché manchiamo in ordine al fotosegnalamento di parecchi immigrati che vengono nel nostro territorio, molti dei quali lasciano perdere le tracce.

Presidente, l'autorità che lei presiede deve tutelare i dati personali. La sua autorità deve intervenire anche laddove il nostro Paese è obbligato ad acquisire, attraverso il fotosegnalamento, dati personali di persone che arrivano nel nostro Paese ? Laddove noi risultiamo inadempienti, voi, come autorità, cosa avete fatto ? Cosa dovremmo fare ? Questo è un problema rilevante.

Peraltro, oggi il *Corriere della Sera* segnala un rimpatrio di molte persone che sono state fotosegnalate, che sono finite poi in altri Paesi, come la Germania, la Svezia, l'Olanda eccetera. Si parla di 15.000 persone che stanno per ritornare. Queste sono persone che sono state fotosegnalate. Laddove questo non è avvenuto, che cosa fa l'autorità che lei presiede ?

ANTONELLO SORO, *Garante per la protezione dei dati personali*. Sono domande complesse.

L'onorevole Brandolin pone una domanda dalla risposta impossibile: qual è il paletto ? Io penso che non esista un punto di equilibrio costante e valido sempre. Conta molto il buon senso. È una categoria del pensiero che ogni tanto si rischia di

smarrire. Occorre evitare di creare un antagonismo fra due cose entrambe importanti: la sicurezza e la *privacy*. Ho provato a dirlo sul PNR.

Il PNR può essere utile ? Io penso che sia utile, ma occorre gestirlo in modo intelligente. Non serve raccogliere il menu che Tizio ha ordinato a pranzo o tutti i menu che vengono ordinati a pranzo da chi viaggia in un volo intercontinentale, perché se un soggetto si sta muovendo con intenzioni malevole sicuramente avrà l'intelligenza di sapere che quel dato viene raccolto e non farà nessuna dieta specifica.

Faccio questo banale esempio per dire che occorre una selezione assolutamente rigorosa dei dati utili e necessari. Se raccogliamo tutti i dati utili rischiamo di replicare il Datagate. Tutto è utile in via teorica. I dati devono essere anche necessari. La raccolta dei dati deve essere governabile e gestibile. Dobbiamo avere la capacità di raccogliere i dati che siamo in grado di tradurre.

Ciò mi lega a un concetto espresso per ultimo dall'onorevole Arrigoni. Se noi raccogliamo molte informazioni, anche fotosegnaletiche, e poi non siamo efficienti nel gestirle, il problema non è raccogliere più informazioni, ma gestire bene quelle che abbiamo.

Si citava l'esempio del caso francese più recente. Lì non c'è stato soltanto il caso della signora che ha preso il volo. Anche gli autori dei delitti di gennaio erano persone segnalate. La questione è: la cooperazione fra le polizie è a un livello elevato quanto servirebbe ? Probabilmente no. Dunque, il problema è renderla efficiente.

Il sistema PNR è un sistema efficiente ? Probabilmente, così come in alcuni Paesi lo hanno creato, se non messo in una rete di cooperazione, non è efficiente. Perché sia efficiente non c'è motivo di creare una gigantesca banca dati in cui abbiamo tutti i dati di tutti coloro che viaggiano. Dobbiamo avere la possibilità di accedere alle compagnie, di chiedere loro i dati essenziali e di farne un uso intelligente.

A mio parere, tutto questo è possibile, ma richiede un grande impegno politico – mi permetto un termine che mi è ormai desueto –, cioè bisogna avere la consapevolezza che la ricerca di questo equilibrio e della protezione dei dati in questa fase è strategica.

Concludo rispondendo all'onorevole Arrigoni, che mi chiedeva cosa facciamo. Noi siamo presenti nell'ambito del coordinamento del *Data Protection Working Party* europeo, che è l'organismo che mette insieme le autorità di protezione dati degli Stati membri. Io sono anche Vicepresidente e svolgiamo una funzione attiva. Abbiamo una riunione settimanale dei nostri uffici.

Lo scambio dei vari gruppi di lavoro nell'ambito europeo è intensissimo. Purtroppo, è tanto intenso da non starci dietro. Noi abbiamo un organico di 140 persone e ne abbiamo al momento poco più di 120 – sono tutti eccellenti giuristi e pochi tecnologi – a fronte di un impegno a livello internazionale che richiederebbero la presenza di tutti. Invece, queste persone ci servono in Italia, per controllare le compagnie telefoniche, le banche, i *call center* e tutto quello che fa parte dell'attività ordinaria di un'autorità che ha un compito di garanzia a 360 gradi, non è un'autorità di regolazione della rete, ma è un'autorità che si occupa di tutto, dal giornalismo fino alla vita in internet.

Cosa possiamo fare nel Nord Africa ? Magari potessimo fare anche noi qualcosa, ma non siamo in condizione di farlo. Noi siamo in condizione di cooperare dentro la rete delle autorità europee, abbiamo dei corrispondenti di riferimento in alcuni Paesi del continente africano e in quasi tutti i Paesi del continente americano. Sta crescendo molto la protezione dati a livello di organizzazione dell'autorità in Asia.

Tuttavia, come è facilmente intuibile, tutto questo avviene in modo sporadico, non organizzato e sistematico, perché c'è un problema di adeguamento delle strutture. Non parlo solo di quella italiana. Quella italiana probabilmente è una di quelle che hanno più difficoltà da questo

punto di vista, ma anche le altre autorità europee hanno numeri, che, rapportati ad autorità di regolazione di rete – non voglio fare comparazioni – sono assolutamente spropositati, pur avendo un ambito di sfide aperte gigantesco.

Per quanto riguarda il Nord Africa, io credo che l'intuizione sia giusta. Può essere importante anche utilizzare in quell'ambito un'attività che favorisca la cooperazione protetta, ma allo stato su questo non c'è niente.

PRESIDENTE. Lei ha fatto un esempio calzante sui due attentatori segnalati in Francia.

Quando siamo stati in ambasciata a Roma, ci hanno spiegato che il tema non era tanto il *data retention* dei dati di questi signori, che erano stranoti alle forze dell'ordine, quanto una legislazione sulle intercettazioni in Francia che non consente assolutamente l'intercettazione di persone legate sentimentalmente ai soggetti individuati dalle forze di polizia come potenziali violatori delle leggi, per attentati o altri crimini. In ambasciata ci hanno spiegato che le fidanzate avevano raccolto dettagli sull'attentato, mentre loro per telefono parlavano del tempo.

LAURA FASIOLO. Vorrei porre un accento particolare sui fatti che sono avvenuti recentemente. Mi riferisco alle due ragazzine invasate che sono state adescate probabilmente attraverso la rete e sono state ritrovate in Turchia con la velleità di portare il loro supporto al jihadismo.

Questi sono problemi non da poco. Credo che un'attenzione particolare debba essere riservata proprio al mondo dell'adolescenza e al mondo della scuola, dove i ragazzi si accostano a queste tecnologie e al *web* in particolare.

La criminalità che si insinua nel *web* è veramente un grosso pericolo. Credo che da questo punto di vista sarebbe bene sensibilizzare più di quanto non si stia facendo il mondo della scuola, perché ci sia una giusta attenzione da parte dei ragazzi e degli adolescenti in particolare a quei fenomeni di adescamento e di *cyber* bullismo che sono pericolosi e rischiano di fagocitare le giovani generazioni e di farle cadere in situazioni così preoccupanti e rischiose.

Un conto è l'obiettivo ideale che noi ci poniamo, un'altra è invece la situazione reale, che è quella che lei ha descritto. Così come l'onorevole Brandolin, anche io sono stata molto colpita da questo dato: il 19 per cento dei dati della pubblica amministrazione, che dovrebbero essere coperti dal *software* NOD, versioni 3, 4, 5 o 6, sono di fatto attaccabili da tutti gli *hacker* possibili.

Si fanno corsi di formazione a raffica nei confronti dei pubblici amministratori per utilizzare dei *software* che poi hanno dei buchi da groviera incredibili. Questo è un altro aspetto.

Da un lato, occorrono attenzione e formazione per quanto riguarda gli adolescenti in particolare e, dall'altro, una formazione ma anche dei *software* e delle misure di protezione che siano veramente efficaci e non così leggere come quelle attualmente in vigore.

ANTONELLO SORO, *Garante per la protezione dei dati personali*. Sono d'accordo. Io penso che l'educazione digitale debba partire dall'ambiente scolastico.

Noi due anni fa proponemmo all'allora Ministro della pubblica istruzione, in modo neanche tanto provocatorio, di far diventare l'educazione digitale materia obbligatoria nelle scuole.

È stato un po' frainteso in quella fase il problema della dotazione di tecnologia a scuola. Non si tratta di dotazione di tecnologia, ma di educazione alla vita nella società digitale, alla conoscenza di tutto quello che significa. È un'esigenza formativa assolutamente ineludibile dai primi anni, anche perché i primi anni di vita dei nostri ragazzi sono già anni di convivenza con la connessione, che sarà sempre più impegnativa, perché la conversione riguarda tutte le cose: gli oggetti, gli elettrodomestici, l'automobile e tutto quello che noi facciamo.

L'altro elemento anch'esso fondativo di una sana politica per la protezione dei dati

è il *privacy by design*. Dal momento in cui tu costruisci un'organizzazione digitale, che sia la banca dati del comune o che sia, invece, la vendita dei frigoriferi e dei televisori intelligenti, deve esserci già in origine un sistema capace di proteggere i dati e di isolare i dati essenziali da quelli che non fanno parte della funzione per la quale li hai raccolti, con meccanismi di cancellazione automatica e un insieme di misure che siano coerenti con la sfida che abbiamo davanti.

Da questo punto di vista, la sfida è destinata a crescere, così come la sensibilità di tutti noi.

Io ho citato l'esempio dei comuni e delle regioni, che sono stati così classificati da una ricerca dell'Università di Roma. Si tratta di una ricerca importante, di un centro di ricerca che ha utilizzato indicatori informatici fra i più attenti.

Potrei dire più banalmente che la cultura della protezione dei dati si scontra con una tendenza in questo momento bulimica alla trasparenza in sede digitale.

In queste settimane – non avete idea di quanto mi dispiaccia – stiamo sanzionando a botte di 10.000 euro ciascuno un'infinità di piccoli comuni italiani che hanno messo in rete le ordinanze di trattamento sanitario obbligatorio dei loro concittadini, con diagnosi, indirizzi e tutti i dati, per un'interpretazione assolutamente in buona fede, ma che non può essere tollerata a questo livello. Ci sono decine di comuni che hanno interpretato la trasparenza.

A questa deformazione concorre anche l'atteggiamento di schizofrenia della cultura italiana che citavo poc'anzi. Adesso c'è la tendenza a mettere tutto in rete. Non tutto va messo in rete. Mettere tutto in rete è rischioso. Io faccio fatica a misurarmi su questo tema anche con alcuni responsabili di altre autorità. Mettere tutto in rete non è trasparenza, ma è molto di più.

Negli Stati Uniti, che vengono citati come esempio, il FOIA *(Freedom of information act)* garantisce il diritto di accesso. Puoi conoscere tutte le informazioni che vuoi, ma le puoi richiedere e le puoi vedere. Metterle in rete, rendendole disponibili a tutto il mondo, è un'altra cosa.

Da questo punto di vista naturalmente il legislatore ha modo anche di ripensare ad alcune norme degli ultimi anni, volendo.

PRESIDENTE. Richiameremo il presidente dell'ANCI, Fassino, per delucidazioni in merito, soprattutto sulla presenza di avvocati nei comuni.

Ringrazio il presidente Soro e dichiaro conclusa la seduta.

La seduta termina alle 10.15.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE
DELLA CAMERA DEI DEPUTATI

DOTT. RENZO DICKMANN

Licenziato per la stampa
il 1º settembre 2015.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

€ 1,00

17STC0011470