

**COMMISSIONE PARLAMENTARE
DI VIGILANZA SULL'ANAGRAFE TRIBUTARIA**

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

19.

SEDUTA DI MERCOLEDÌ 25 MARZO 2015

PRESIDENZA DEL PRESIDENTE GIACOMO ANTONIO PORTAS

INDICE

<p>Sulla pubblicità dei lavori:</p> <p style="padding-left: 20px;">Portas Giacomo Antonio, <i>Presidente</i></p> <p>INDAGINE CONOSCITIVA SULL'ANAGRAFE TRIBUTARIA NELLA PROSPETTIVA DI UNA RAZIONALIZZAZIONE DELLE BANCHE DATI PUBBLICHE IN MATERIA ECONOMICA E FINANZIARIA. POTENZIALITÀ E CRITICITÀ DEL SISTEMA NEL CONTRASTO ALL'EVAZIONE FISCALE^{PAG.}</p>	<p>3</p>	<p>Audizione del presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro:</p> <p style="padding-left: 20px;">Portas Giacomo Antonio, <i>Presidente</i> 3, 6, 11</p> <p style="padding-left: 20px;">Bellot Raffaella (LNA) 9, 10</p> <p style="padding-left: 20px;">Bignami Laura (Misto-Movimento X) 8, 10</p> <p style="padding-left: 20px;">Soro Antonello, <i>presidente dell'Autorità garante per la protezione dei dati personali</i> 3, 6, 8, 10</p> <p style="padding-left: 20px;">Sposetti Ugo (PD) 7</p>
---	----------	--

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE
GIACOMO ANTONIO PORTAS

La seduta comincia alle 8.30.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata mediante l'attivazione del sistema audiovisivo a circuito chiuso e la trasmissione diretta sulla *web-tv* della Camera dei deputati e, successivamente, sul canale satellitare della Camera dei deputati.

Audizione del presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro.

PRESIDENTE. L'ordine del giorno reca l'audizione del presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro, che, anche a nome dei colleghi, ringrazio per aver accolto l'invito della Commissione. Sono presenti, inoltre, Mario De Bernart, dirigente servizio relazioni istituzionali, Claudio Filippi, dirigente dipartimento libertà pubbliche e sanità, e Baldo Meo, dirigente servizio relazioni con i mezzi di informazione.

L'audizione si inquadra nell'ambito dell'indagine conoscitiva sull'anagrafe tributaria nella prospettiva di una razionalizzazione delle banche dati pubbliche in materia economica e finanziaria. Potenzialità e criticità del sistema nel contrasto all'evasione fiscale.

Do la parola al presidente Soro, con riserva per me e per i colleghi di rivolgergli, al termine del suo intervento, domande e richieste di chiarimenti.

ANTONELLO SORO, *presidente dell'Autorità garante per la protezione dei dati personali*. La realizzazione di un moderno e efficiente sistema fiscale, un'effettiva semplificazione dei rapporti con i contribuenti, un'azione di contrasto all'evasione costituiscono un interesse generale rispetto al quale naturalmente esiste — non può che essere così — il massimo dell'attenzione e della collaborazione dell'Autorità per la protezione dei dati personali. Appare del tutto evidente che le disposizioni legislative che nel tempo hanno implementato i compiti e le modalità di funzionamento dell'Agenzia delle entrate hanno determinato la creazione di flussi ingenti di dati personali e hanno consentito a una pluralità di soggetti di accedere ai dati stessi. La crescente esigenza di condividere queste informazioni ha, dunque, determinato un impatto rilevante in tema di protezione dei dati personali particolarmente delicati quali quelli riferiti ai contribuenti.

Nell'esercizio della nostra funzione consultiva, ci siamo sempre impegnati nella ricerca di un ponderato punto di equilibrio fra l'obiettivo dell'equità fiscale, che è la finalità principale di molte di queste norme, e la tutela di un diritto fondamentale, come quello alla protezione dei dati personali, riconosciuto dal Trattato di Lisbona e ormai assorbito dalla Costituzione italiana, con l'intento di difendere i diritti, e di rendere più efficienti i sistemi in cui i dati sono conservati.

Nella considerazione di indiscutibile legittimità delle finalità perseguite dall'amministrazione, abbiamo sempre evidenziato la necessità di coniugare l'efficacia dei provvedimenti con l'acquisizione delle sole informazioni indispensabili allo scopo, impiegando modalità di trattamento pro-

porzionate, piuttosto che una indifferenziata, preventiva e generalizzata acquisizione dei dati, senza che ciò sia realmente necessario. Le banche dati di cui si compone oggi il sistema della fiscalità sono tali da assicurare un notevole patrimonio informativo disponibile per le amministrazioni. Per questo, pensiamo che adesso sia opportuno potenziarne la capacità di gestione e di utilizzo, affinché siano realmente efficaci, garantendo, ad esempio, l'omogeneità e l'univocità nella raccolta e nella classificazione dei dati. La sola quantità e l'estensione del patrimonio informativo non assicurano necessariamente la funzionalità del sistema.

Nel corso di questi anni l'attività del Garante si è articolata proprio nella verifica e nella prescrizione di tutte le misure di sicurezza relative ai sistemi di archiviazione, ai flussi di dati, alla interoperabilità delle diverse banche dati detenute e condivise tra le amministrazioni dello Stato, gli enti locali, gli organismi di previdenza, i patronati e le varie agenzie. Ormai questo insieme di banche dati è diventato una struttura strategica del Paese. Proteggere i dati ivi conservati consente non solo di tutelare i diritti dei cittadini, ma ha soprattutto l'obiettivo di tutelare la sicurezza del sistema.

Mi preme evidenziare che i numerosi provvedimenti adottati dal Garante in questi anni, spesso anche all'esito di accertamenti di carattere ispettivo, sono stati il frutto di una proficua attività di collaborazione e condivisione svolta con l'Agenzia delle entrate, che ha sempre recepito le nostre indicazioni prescritte nel tempo. È il caso del recente parere del 19 febbraio scorso riferito al modello 730 precompilato, che si inserisce nell'ottica di una maggiore semplificazione fiscale che inverte i rapporti tra fisco e cittadino. L'Autorità ha attivamente collaborato alla precisazione delle modalità tecniche del sistema, definite con un provvedimento del direttore dell'Agenzia delle entrate e destinate a proteggere una rilevante quantità di informazioni contenute nel modello precompilato e nell'elenco dei documenti a esso attinenti. In particolare, i correttivi

introdotti dall'Agenzia delle entrate su nostra richiesta hanno consentito di evitare che i dati dei contribuenti potessero essere accessibili per il solo tramite del loro codice fiscale ovvero utilizzando il PIN proprio da parte dei soggetti autorizzati. Al fine di poter avanzare all'Agenzia la richiesta di accesso a una o più dichiarazioni precompilate, i soggetti autorizzati dovranno essere in possesso, oltre che del codice fiscale, di una specifica delega, compreso il numero e il tipo di documento del contribuente delegante, proprio a garanzia dell'effettivo conferimento della delega stessa, che dovrà essere numerata e datata, e di altre puntuali informazioni desunte dalla dichiarazione relativa all'anno precedente quali, ad esempio, il reddito complessivo. È previsto che l'Agenzia provveda a richiedere a campione copia delle deleghe e dei documenti indicati nelle richieste di accesso, che dovranno essere trasmessi entro 48 ore. I soggetti autorizzati potranno visualizzare esclusivamente le dichiarazioni precompilate richieste e l'accesso alle stesse dovrà essere preceduto dalla digitazione di un codice di sicurezza, al fine di evitare l'utilizzo di « robot » per un accesso massiccio ai servizi offerti dall'Agenzia. Il contribuente, al fine di garantire una maggiore trasparenza, potrà visualizzare l'elenco dei soggetti ai quali la sua dichiarazione precompilata è stata messa a disposizione.

Per quanto attiene alla sicurezza dei canali telematici utilizzati, l'Agenzia dovrà tracciare gli accessi ai sistemi telematici dell'Anagrafe tributaria da parte di ciascun soggetto autorizzato e dovrà predisporre strumenti di monitoraggio e analisi periodica degli stessi, attivando specifiche allerte per individuare comportamenti anomali o a rischio. Particolarmente importante è la prescrizione rivolta all'Agenzia di garantire la cifratura dei dati trasmessi, nonché il limite temporale, fissato al 10 novembre, oltre il quale non sarà più disponibile la possibilità di accedere alle dichiarazioni precompilate. L'Agenzia ha inoltre comunicato di voler avviare un tavolo di confronto con gli intermediari,

per rafforzare ulteriormente le misure di sicurezza del canale utilizzato. Quanto ai dati sanitari, si fa presente che solo con riferimento all'anno 2016 è previsto che il sistema tessera sanitaria metta a disposizione dell'Agenzia le spese sanitarie sostenute dai cittadini nell'anno 2015.

L'obiettivo del Garante, che a breve sarà chiamato a esprimere un parere sul punto e i cui uffici, peraltro, nel pomeriggio di oggi svolgeranno un incontro tecnico con i rappresentanti del Ministero dell'economia, dell'Agenzia, della SOGEI e del Ministero della salute, sarà quello di verificare che le informazioni necessarie all'Agenzia per la predisposizione della dichiarazione precompilata non contengano dati sul dettaglio delle prestazioni sanitarie o dei farmaci erogati.

A proposito del precompilato, abbiamo avuto notizia dai resoconti che in questa sede si è più volte fatto cenno a un'intempestività — usiamo un eufemismo — dell'Autorità garante rispetto al parere, che avrebbe rallentato l'entrata a regime del modello precompilato. Voglio ricordare, senza voler fare polemiche, che il decreto legislativo su cui si fonda il modello precompilato è datato 21 novembre 2014. Soltanto il 30 gennaio 2015, oltre due mesi dopo, l'Agenzia delle entrate, che credo avesse concorso nell'elaborazione del decreto stesso, ha trasmesso al Garante la richiesta di un parere. Il Garante ha immediatamente attivato un tavolo con i funzionari, rilevando l'assoluta inadeguatezza del solo dato codice fiscale quale titolo di accesso ai dati contenuti nella banca dati. Il nuovo schema, alla luce delle nostre raccomandazioni, interamente raccolte e condivise, è stato inoltrato in data 13 febbraio e il 19 febbraio l'Autorità ha espresso il relativo parere formale. Essendo un organo collegiale, è evidente che non può essere adottato il parere la mattina stessa in cui arriva un decreto. In venti giorni abbiamo ottenuto l'adeguamento dei testi dello schema alle richieste avanzate. Dire che questo è un parere che arriva in ritardo mi sembra quantomeno ingeneroso.

Oltre all'obiettivo di perseguire una maggiore semplificazione fiscale, abbiamo collaborato per potenziare i sistemi informativi dell'Anagrafe tributaria tesi a un più efficace contrasto all'evasione fiscale. Mi riferisco agli interventi del Garante sulla cosiddetta « Anagrafe dei conti » e in particolare al parere reso nel novembre 2012, relativo agli obblighi delle banche e degli operatori finanziari di comunicare annualmente all'Agenzia, ai fini di controllo fiscale, anche le informazioni sulle movimentazioni relative ai conti correnti bancari dei cittadini. L'Autorità ha più volte evidenziato che l'esigenza di disporre di informazioni considerate utili per realizzare un interesse costituzionalmente protetto non può essere messa in discussione. Si è, tuttavia, ribadito che le informazioni raccolte dall'Anagrafe dei conti potranno essere trattate esclusivamente per la realizzazione, sulla base di specifici criteri predefiniti, di analisi del rischio di evasione. Nel rispetto di questa finalità, che impedisce di fatto un controllo generalizzato e diffuso di tutti i contribuenti, lo sforzo principale è stato quello di definire stringenti misure di sicurezza di natura tecnica, quali ad esempio la non intelligibilità dei dati, e organizzativa, come l'autenticazione e la tracciabilità degli accessi al sistema nonché specifici profili di autorizzazione dei soggetti, che devono essere un numero limitato, selezionato e tracciabile, a garanzia della protezione dei dati in fase di trasmissione, di accesso e di conservazione. Abbiamo previsto per gli operatori finanziari e le banche: l'obbligo di adottare meccanismi di cifratura dei dati, al fine di scongiurarne il rischio di alterazione; l'adozione di protocolli sicuri per eventuali trasmissioni interne all'operatore finanziario; limitato accesso ai *file* per un numero ristretto di incaricati legittimati in ragione delle mansioni svolte; aggiornamento costante dei sistemi operativi e dei *software* antivirus e antintrusione; eventuale conservazione dei dati solo in forma cifrata.

Tra gli adempimenti prescritti all'Agenzia delle entrate, rilevano la predisposizione di canali telematici adeguati alla

comunicazione di un'elevata quantità di dati, privilegiando l'interconnessione diretta con i sistemi informativi di banche e istituti finanziari, e l'obbligo di fornire agli operatori finanziari indicazioni e accorgimenti per la predisposizione dei *file* da inviare. Si è inoltre ravvisata l'esigenza di specificare i tempi di conservazione dei dati presso l'Anagrafe, ossia sei anni, quale termine massimo, perché siano poi cancellati integralmente in maniera automatica. Si fa presente che la trasmissione dei suddetti dati contabili non avviene per il tramite del servizio telematico Entratel, inizialmente individuato, che presentava diverse criticità, ma mediante una nuova infrastruttura informatica, il sistema di interscambio dati (SID), che consente la realizzazione di procedure di trasmissione totalmente automatizzate, riducendo quindi la possibilità di un utilizzo illegittimo dei dati rispetto alle trasmissioni manuali. È opportuno evidenziare che le predette informazioni che arrivano all'Anagrafe tributaria si dovranno arricchire a breve di nuovi dati, allo scopo principale di determinazione dell'ISEE, quali quelli relativi al valore medio di giacenza annua di depositi e conti correnti bancari e postali. Anche il relativo decreto del direttore dell'Agenzia è stato inviato il 16 marzo all'Autorità per il previsto parere.

Per ultimo, pensiamo che sia stato di particolare importanza il ruolo svolto dal Garante nell'ambito di una richiesta di verifica preliminare con riferimento al nuovo redditometro. L'intervento incisivo dell'Autorità ha in particolare consentito di eliminare l'individuazione di criteri astratti, volti ad analizzare il comportamento del contribuente, effettuata sulla base delle numerose tipologie di dati posseduti e attraverso l'attribuzione di un profilo. Il Garante ha ritenuto che il decreto ministeriale, nella parte in cui prevedeva la profilazione del contribuente attraverso l'imputazione presuntiva di elementi di capacità contributiva relativi a ogni singolo aspetto della vita quotidiana, costituiva un'ingerenza ingiustificata nella vita privata degli interessati, in quanto

sproporzionata rispetto alle legittime finalità di interesse generale perseguite dall'Agenzia. Alle luce di questa considerazione, ha prescritto all'Agenzia di ricostruire il reddito del contribuente utilizzando unicamente spese certe e non i dati delle spese medie Istat, così com'era in origine. Questa nostra indicazione è stata naturalmente condivisa e implementata anche con la valutazione conclusiva dell'Agenzia delle entrate di un risultato positivo per la stessa efficienza del sistema.

Mi fermo qui, riassumendo il concetto che le banche dati detenute dall'Agenzia delle entrate sono uno dei contenitori più delicati di informazioni, non solo fondamentali per i cittadini contribuenti, ma strategiche nell'interesse generale del Paese, e che la violabilità delle banche dati costituisce oggi una vera emergenza rispetto alla minaccia cibernetica. Rispetto alla minaccia cibernetica, che mette in discussione la sicurezza reale del Paese, proteggere le banche dati dell'Agenzia delle entrate, come le altre banche dati strategiche, non è semplicemente un tributo di attenzione e di sensibilità al tema *privacy*, ma è una misura e un presupposto di sicurezza dello Stato. Vorrei che questo fosse chiaro, per comprendere che tutte le misure di sicurezza da noi proposte avevano e hanno esclusivamente l'obiettivo di mettere in sicurezza il sistema e di renderlo efficiente. Una banca dati violabile non è efficiente. La missione di contrasto all'evasione fiscale verrebbe assolutamente messa in discussione dalla vulnerabilità del sistema stesso.

PRESIDENTE. Capisco che suddividere in due parti il PIN per i cittadini sia giustamente teso verso l'obiettivo relativo alla *privacy* cui lei accennava, ma non si poteva immaginare di mandare a casa dei cittadini una classica lettera con il tessero, come fanno per le carte di credito, con un PIN, invece di suddividerlo in due parti?

ANTONELLO SORO, presidente dell'Autorità garante per la protezione dei dati personali. C'è un punto fondamentale. Nel

decreto sottoposto al nostro esame si ipotizzava l'utilizzo di due strumenti: codice fiscale e/o il PIN affidato al CAF o al cittadino. Sia il cittadino sia il CAF, una volta che entrano in possesso di un unico elemento di identificazione attraverso il quale accedere alla banca dati, entrano in possesso di uno strumento che vale anche in futuro. È ragionevole immaginare infatti che il sistema costruito per la pre-compilata non sia destinato a durare un solo anno, ma anche per il futuro. Per questa ragione, l'atto di delega da parte del cittadino nei confronti del professionista o del CAF deve rinnovarsi per consentire l'accesso alla banca dati esclusivamente a chi ne ha titolo.

La delega, che costituisce il presupposto della titolarità del CAF, del commercialista o di chiunque altro ad accedere ai dati, deve essere documentata. Il CAF se non ha la disponibilità della delega non potrà in alcun modo accedere alla banca dati. Per le ragioni che ricordavo prima, si impedisce di fatto l'accesso di un « curiosone » che ha voglia di guardare la dichiarazione dei redditi del vicino di casa, dovendo peraltro detto accesso essere tracciabile. Il professionista che accede alle banche dati in Italia deve sapere che sta compiendo un atto di grande responsabilità. Pertanto, offrire esclusivamente un elemento di identificazione per accedere a questa banca dati è insufficiente. Deve essere documentata e conservata la delega, tracciato l'ingresso del singolo professionista e offerta la possibilità al cittadino di sapere chi ha consultato i suoi dati. Se il cittadino dovesse scoprire che sono andati a guardarlo anche professionisti o CAF diversi da quelli legittimati dalla delega hanno avuto accesso ai suoi dati, scatterebbe un meccanismo di allarme. Complessivamente il sistema, così come proposto, era assolutamente labile e vulnerabile. Pensiamo di aver introdotto un elemento di maggiore sicurezza. Naturalmente non esiste mai un'assoluta sicurezza dei sistemi informatici, ma dobbiamo assumere la protezione dei sistemi informatici come una scelta strategica. Da questo punto di vista, prendo atto che l'Agenzia delle entrate ha

condiviso le nostre valutazioni e si è adeguata. Non abbiamo mai registrato una divergenza. I nostri uffici hanno avuto un confronto anche in tante altre passate occasioni. Ci siamo confrontati arrivando a un punto di condivisione. Immagino che questo sia anche un segno di ragionevolezza delle proposte che noi abbiamo fatto.

La SOGEI oggi rischia di essere un bersaglio tra i più importanti del nostro Paese. Non c'è un punto di attacco più delicato rispetto a qualunque altra banca dati italiana: credo che proteggerla sia un interesse prima di tutto dell'Agenzia delle entrate, oltre che del Governo e del Parlamento.

UGO SPOSETTI. Condivido molto la parte della relazione del presidente e la risposta che è stata data sulla protezione dei dati sensibili dei cittadini italiani. Penso che debba essere fatto uno sforzo per il futuro immediato, perché ormai la nostra vita privata non esiste più. A parte l'invio all'Agenzia delle entrate, i conti correnti di persone politicamente esposte hanno un trattamento diverso da quelli di tutti gli altri cittadini. Questo può essere anche giusto. Per quanto concerne le protezioni che sono state riferite dal presidente Soro, è evidente che non sono mai garantite al 100 per cento, quindi va fatto uno sforzo *in progress*. Si proteggono i dati e vi è chi studia sistemi per inserirsi e viceversa.

Non c'entra nulla, però, presidente Portas e presidente Soro, io, come avete visto leggendo i giornali, sono stato oggetto di divulgazione di mie conversazioni telefoniche. La cosa simpatica che mi è capitata è che nei brogliacci delle conversazioni telefoniche è rimasto in evidenza il numero del mio cellulare. Potete immaginare cosa sai successo. Questo non mi crea nessun disturbo: rispondo o, se non posso, richiamo, perché ho una educazione all'antica.

Tuttavia, penso che tutto questo andrebbe evitato: capisco l'esigenza di far circolare le informazioni, però ci mancava solo che evidenziassero l'indirizzo di casa! È un fatto che intendo segnalare all'atten-

zione del presidente dell'Autorità garante, perché non mi pare che sia un modello di vita di una società avanzata.

LAURA BIGNAMI. Ringrazio per la relazione. Per quanto riguarda il codice di accesso, credo che l'uso del codice fiscale non fosse comunque tecnicamente possibile e fosse una scelta bocciabile a priori. Per quanto concerne la possibilità di individuare chi ha fatto l'accesso alla mia utenza, si vede il CAF o la persona fisica? Non penso che l'identificazione sia personale. Suppongo sia identificato solo il centro.

Immagino che la protezione ordinaria dei dati comporterà delle spese. Chiedo se ci sono invece investimenti sugli attacchi straordinari, vista la nostra posizione internazionale un po' delicata di questo periodo.

ANTONELLO SORO, *presidente dell'Autorità garante per la protezione dei dati personali*. Vorrei dire al senatore Sposetti che sono assolutamente sensibile alla sua sollecitazione. Il tema coinvolge responsabilità diverse, a partire da quelle del Parlamento, dell'Ordine dei giornalisti e naturalmente anche del Garante.

Abbiamo già sollevato la questione con riferimento alla pubblicazione impropria di un indirizzo personale, che ha riguardato personalità politiche, dell'alta amministrazione e del mondo dello spettacolo. In alcuni casi abbiamo proceduto con interventi sanzionatori e con istruttorie concluse con la dichiarazione di illiceità riferita alla pubblicazione di informazioni ritenute assolutamente eccedenti rispetto all'interesse pubblico che presiede alla libertà di informazione e alla sua tutela.

Esiste però un problema più generale. Non sono convinto che non esista più la *privacy* dei cittadini: si tratta di un diritto fondamentale e una democrazia che si rassegni all'idea che i diritti fondamentali vengono calpestati, sarebbe una democrazia declinante. Si tratta di assumere una più matura responsabilità da parte di tutti. Abbiamo perseguito la strada di un aggiornamento del codice deontologico dei

giornalisti — mi rendo conto che si tratta di argomento un po' estraneo all'ordine del giorno della Commissione, ma il senatore Sposetti ha posto il problema e io ho il dovere di rispondere.

Abbiamo chiesto espressamente, ai sensi della vigente normativa che ci dà facoltà di promuovere il codice deontologico dei giornalisti, di aggiornarlo e per sei mesi ci siamo incontrati con i delegati dell'ordine e con la presidenza. Abbiamo elaborato alcune ipotesi di graduale modifica, non di radicale ribaltamento, consapevoli di confrontarci su un terreno assolutamente delicato, caratterizzato dalla presenza di due diritti tutelati dalla Costituzione, la libertà di informazione e la tutela del diritto alla dignità personale. La *privacy* è infatti un nome della libertà che coincide con la tutela della dignità della persona, fondamento della Costituzione italiana e uno dei fondamenti della Costituzione europea secondo il trattato di Lisbona e la Carta di Nizza.

In queste materie, la delicatezza impone una ricerca equilibrata: abbiamo condiviso con la presidenza dell'ordine dei giornalisti una ipotesi di nuovo codice ma in sede di consiglio nazionale l'ordine non ha voluto ratificare la bozza elaborata. Il collegio dell'Autorità garante si è rifiutato di esercitare il potere sostitutivo che pure la legge ci attribuisce, perché un codice deontologico non può essere frutto di un atto d'imperio: non può esserci una autorità che impone il codice deontologico. Se si deve procedere di imperio spetta al Parlamento trovare un diverso punto di equilibrio. Certo è che alla sensibilità verso questi problemi corrisponde la cultura del « nimby » (*not in my back yard*), cioè si è molto sensibili alla *privacy* e alla protezione della propria dignità personale, quando appunto ci riguarda personalmente, si è totalmente indifferenti quando riguarda quella degli altri e forse si tratta di un problema culturale del nostro Paese sul quale ognuno di noi dovrà fare la sua parte.

Penso tuttavia che il problema da lei posto non sia irrilevante rispetto al tema generale della sicurezza delle banche dati.

Siamo in tempi in cui una certa bulimia di trasparenza della pubblica amministrazione sta portando a mio parere a una non sufficiente valutazione della immissione in rete di una infinità di informazioni personali riferite non semplicemente ai parlamentari o agli uomini di governo, ma a un numero elevato di cittadini che hanno semplicemente una qualche titolarità di incarichi pubblici. Per fare un esempio, uno studente che entra nel senato accademico rispetto al Presidente del Consiglio forse ha qualche ragione in meno di avere i dati attinenti al suo patrimonio e a quello dei parenti fino al secondo grado, pubblicati in rete.

La rete, rispetto alla conoscibilità precedente alla società digitale, è un'altra cosa; un dato in rete significa che la propria identità e le proprie informazioni possono essere rubate per costruire un'altra identità digitale, mettendo in gioco reputazione, portafoglio e la propria vita!

Colgo dunque l'occasione per segnalare a questa Commissione, composta da deputati e senatori, un supplemento di attenzione al bilanciamento tra l'esigenza sana e giusta della trasparenza con quella della protezione della vita dei cittadini, perché la protezione dei dati ha questo significato. Non mi addentro ulteriormente nel merito di un discorso che peraltro mi appassiona molto, ma su questo tema un supplemento di riflessione pubblica sarebbe opportuno.

Rispondo brevemente rispetto al quesito della senatrice Bignami. L'informazione che viene registrata è quella dell'operatore che, attraverso un CAF, ha avuto accesso. Il CAF ha una sua identificabilità, ma all'interno di quel CAF va registrato l'operatore che ha fatto l'intervento e l'accesso. Qui si pone un problema. Non ne abbiamo discusso tanto neanche noi, perché alla fine bisognava rendere il parere, il cui ritardo, ribadisco, non era dovuto comunque alla nostra Autorità. È previsto che i dati del CAF di Torino vengano trasmessi alla banca dati centrale del CAF che ha operato il trattamento di questi dati. Effettueremo — credo a breve — alcune ispezioni nei

confronti dei principali CAF italiani, perché naturalmente il livello di protezione di quelle banche dati diventa anch'esso un punto di vulnerabilità importante. Bisogna identificare bene la struttura e, dentro la struttura, l'operatore: sono dati molto delicati. Nella denuncia dei redditi c'è molto della nostra vita, quindi è bene che tutti questi dati siano adeguatamente protetti.

Gli investimenti sono esattamente l'altra faccia della medaglia dell'Agenda digitale. Si può pensare che la digitalizzazione della pubblica amministrazione sia un elemento di efficienza del sistema e nessuno può mettere in dubbio che questo sia un obiettivo, ma se costruiamo una banca dati della pubblica amministrazione non protetta, faremmo un danno enorme alla pubblica amministrazione, al sistema e alla strategia difensiva del Paese.

Un recente studio dell'Università la Sapienza di Roma ha evidenziato che lo stato di protezione delle banche dati delle ASL, delle regioni e dell'amministrazione centrale, con vario grado, è totalmente inadeguato rispetto all'esigenza di protezione moderna delle banche dati che contengono informazioni più o meno delicate. Alcune sono molto delicate e altre meno, ma tutte complessivamente concorrono a mettere a repentaglio il sistema. Pertanto, gli investimenti sono assolutamente urgenti. Per fare investimenti, occorre però che ci sia una consapevolezza, che spetta a tutti quelli che hanno responsabilità.

RAFFAELA BELLOT. Grazie per l'esposizione, ma anche per la parte in cui si è vista una ricerca personale su un problema che riguarda i cittadini in entrambe le situazioni: l'uso dei propri dati e l'indifferenza nell'uso di quelli degli altri. È anche un problema di natura etica, che sicuramente dovremmo tutti quanti acquisire. Vorrei sapere come vengono verificate le capacità dei professionisti, dei CAF e di chi gestisce i dati, a garanzia del fatto che questi dati non siano accessibili. Ha già parzialmente risposto alla mia collega. Come farete a verificare a campione, come diceva lei, l'attendibilità dei CAF? Nel caso in cui sia verificata questa incapacità di

gestire i dati, come sarà l'approccio? Questi CAF o questi professionisti avranno indicazioni o saranno sollevati temporaneamente dal potere di utilizzare le banche dati? Come funzionerà? Un conto è verificare l'inefficienza del professionista e un conto è agire nel caso in cui lo si riscontri.

Lei parlava, se ho ben inteso, di sei anni per la conservazione delle deleghe. Considerando il tempo per la lavorazione dei modelli fiscali, l'accesso e l'utilizzo di dati da parte del professionista, eventuali ricorsi ed errori, sei anni è un termine congruo, valutato su una logica temporale, oppure è fissato sulla base di altri motivazioni?

ANTONELLO SORO, *presidente dell'Autorità garante per la protezione dei dati personali*. Parto dall'ultima domanda. Il tempo di conservazione dei dati è commisurato al termine massimo di decadenza previsto in materia di accertamento delle imposte sui redditi. Naturalmente si può concludere prima.

RAFFAELA BELLOT. La mia domanda era conseguente al fatto che lei diceva che il cittadino può eventualmente verificare l'utilizzo delle deleghe o chi ha avuto accesso. Se il fatto è antecedente ai sei anni, ovviamente non avrà più modo di capire. La mia domanda era nel senso della tutela del cittadino che vuole capire perché sei anni prima qualcuno ha avuto accesso ai suoi dati. Purtroppo la temporalità in questi casi cambia.

ANTONELLO SORO, *presidente dell'Autorità garante per la protezione dei dati personali*. Come sempre accade, i tempi di conservazione delle informazioni in tutte le banche dati devono avere comunque un limite. Si è ritenuto che sei anni fosse il tempo congruo come termine massimo, perché è lo stesso termine di decadenza. Il tempo di allerta che l'Agenzia dovrebbe avere introdotto nel sistema informatico consente di sapere se ci sono accessi sospetti, il che è già importante. Il cittadino che dovesse avere qualche problema

presumibilmente nell'ambito di un periodo di sei anni si chiederà chi ha avuto accesso ai suoi dati e avrà la possibilità di saperlo. Un po' di attenzioni in questo senso ci sono. Può darsi che siano sufficienti o che vadano ripensate, ma noi e l'Agenzia riteniamo che queste misure al momento siano di facile governo e anche approntamento. Altrimenti, se introducessimo misure più complesse, queste comporterebbero tempi ancora maggiori.

Per quello che riguarda, invece, il profilo dei CAF che dovessero avere un comportamento non adeguato, ci sono due garanzie: le ispezioni, che intendiamo effettuare, e il sistema delle allerte che la stessa Agenzia implementerà. Naturalmente il CAF ha un rapporto convenzionale con l'Agenzia delle entrate. Se accertiamo che un CAF ha compiuto un illecito, per parte nostra c'è l'apparato sanzionatorio del Codice della *privacy* e della protezione dei dati personali, mentre da parte dell'Agenzia delle entrate ragionevolmente ci può essere lo strumento più alto della risoluzione della convenzione. Se creiamo meccanismi di reciprocità, di controllo e di monitoraggio, comprese le ispezioni a campione che l'Agenzia si è impegnata a fare e ha previsto di poter fare, creiamo un meccanismo che tendenzialmente porta verso l'efficienza e anche verso la legalità del sistema complessivo. Tutto questo andrà verificato e credo che, mai come in questo campo, ci sia bisogno di tenere alta l'attenzione.

LAURA BIGNAMI. Una curiosità. Le ispezioni a campione, di cui parlava poc'anzi, rispettano dei principi o sono esclusivamente casuali? Non voglio che me li dica, però spero ci siano criteri logici e che non siano solo rimesse al caso.

ANTONELLO SORO, *presidente dell'Autorità garante per la protezione dei dati personali*. Per quanto concerne le ispezioni a campione fatte dall'Agenzia delle entrate, sarà quest'ultima che si darà una sua regola.

Le ispezioni che noi ci proponiamo di effettuare e che effettuiamo periodica-

mente sulla stessa Agenzia delle entrate, oltre che su altre banche dati pubbliche e private, sono disciplinate da criteri vari, non certamente punitivi nei confronti di qualcuno, ma basati sull'esperienza che periodicamente viviamo.

La nostra è una Autorità complessa, che si occupa di grandi questioni. Ci occupiamo di *Google*, ma anche del cittadino che ha un problema personale e che giustamente si rivolge all'istituzione preposta. Molto spesso la Guardia di finanza registra un illecito reale o potenziale nel trattamento dei dati personali e ce lo segnala. Noi andiamo a verificare e scopriamo inefficienze, che da piccole poi possono diventare grandi.

Sul caso specifico, mi riprometto — ne ho parlato con gli uffici — di prestare una grande attenzione sulle modalità con cui i CAF gestiscono, conservano e trattano i

dati perché lì si concentrano informazioni che devono essere davvero protette. Il sistema, così come lo abbiamo registrato, su questo punto probabilmente ha qualche carenza: si tratta del primo anno ma cercheremo comunque di impegnarci.

PRESIDENTE. Ringrazio il presidente Soro e i suoi collaboratori e dichiaro conclusa l'audizione.

La seduta termina alle 9.15.

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

DOTT. VALENTINO FRANCONI

*Licenziato per la stampa
il 17 aprile 2015.*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO



17STC0009151