

**COMMISSIONE PARLAMENTARE
DI VIGILANZA SULL'ANAGRAFE TRIBUTARIA****RESOCONTO STENOGRAFICO****INDAGINE CONOSCITIVA**

9.

SEDUTA DI MERCOLEDÌ 7 LUGLIO 2021PRESIDENZA DEL PRESIDENTE **UGO PAROLO****INDICE**

	PAG.		PAG.
Sulla pubblicità dei lavori:		Cantone Carla (PD)	10
Parolo Ugo, <i>presidente</i>	2	De Bertoldi Andrea (FdI)	7
INDAGINE CONOSCITIVA «DIGITALIZZAZIONE E INTEROPERABILITÀ DELLE BANCHE DATI FISCALI»		Fenu Emiliano (M5S)	9
Audizione del presidente dell'Autorità garante per la protezione dei dati personali, Pasquale Stanzione:		Marino Mauro Maria (IV)	8
Parolo Ugo, <i>presidente</i>	2, 7, 10, 11	Stanzione Pasquale, <i>presidente dell'Autorità garante per la protezione dei dati personali</i>	2, 10

PRESIDENZA DEL PRESIDENTE
UGO PAROLO

La seduta comincia alle 8.35.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata mediante l'attivazione dell'impianto audiovisivo a circuito chiuso e la trasmissione in diretta *streaming*, con modalità sperimentale, sulla *web tv* della Camera dei deputati.

Audizione del presidente dell'Autorità garante per la protezione dei dati personali, Pasquale Stanzone.

PRESIDENTE. L'ordine del giorno reca l'audizione del presidente dell'Autorità garante per la protezione dei dati personali, professor Pasquale Stanzone, supportato dalla direttrice del Servizio affari legislativi e istituzionali, avvocatessa Federica Resta, ai quali do il benvenuto.

Come è noto ai nostri convenuti, la Commissione mira ad acquisire l'apporto del Garante sul tema degli ostacoli (evidenziati in particolare nell'audizione del direttore dell'Agenzia delle entrate dello scorso 5 maggio) che possano essere rappresentati dall'applicazione delle norme in materia di protezione dei dati personali alla realizzazione del cosiddetto principio *once only*, per il quale la pubblica amministrazione non dovrebbe chiedere al cittadino informazioni di cui già dispone.

Sarà inoltre gradito ogni contributo che il professore e l'avvocato riterranno di poter rendere in ordine alle eventuali criticità in tema di trattamento dei dati personali

che possano derivare dallo sviluppo della digitalizzazione e dell'interoperabilità delle banche dati della pubblica amministrazione.

Prima di cedere la parola al professor Stanzone avverto che, oltre all'onorevole Cantone che è presente, sono collegati la vicepresidente, senatrice Gaudiano, il senatore Fenu, il senatore Marino e l'onorevole Giacometto che sono collegati da remoto. Cedo, quindi, la parola al professor Stanzone, che ringrazio per la sua disponibilità e per la presenza. Prego, professore.

PASQUALE STANZIONE, *presidente dell'Autorità garante per la protezione dei dati personali*. Grazie, presidente. Io ringrazio la Commissione per questo confronto su di un tema, oggetto dell'indagine conoscitiva, di rilievo centrale, soprattutto alla luce dell'importanza ascrivibile nell'ambito delle riforme correlate al Piano Nazionale di Ripresa e Resilienza (PNRR).

La digitalizzazione delle banche dati pubbliche è un processo che sicuramente ora è nella fase del suo più accentuato sviluppo, ma che non è certo nuovo e che, anzi, ha rappresentato spesso l'occasione per un dialogo proficuo tra Garante e Governo, soprattutto con riferimento alla materia fiscale.

L'obiettivo, in gran parte realizzato, di questo confronto è stato sempre quello di delineare le condizioni migliori per rendere l'azione di contrasto dell'evasione e dell'evasione fiscale tanto più efficace, quanto più conforme a quelle garanzie sostanziali e procedurali di correttezza e di sicurezza che la disciplina della *privacy* prevede anche in questo ambito.

Qualche incomprendimento ha indubbiamente caratterizzato la dialettica tra l'Autorità e il Governo sul punto ed è, a mio avviso, riconducibile a una non corretta

rappresentazione della *privacy* come ostacolo, inutile fardello di cui si vorrebbe gravare l'amministrazione finanziaria, ma che invece si è dimostrata ed è un necessario presupposto di efficacia e di corretto svolgimento dell'azione di contrasto degli illeciti fiscali.

Nel garantire, in particolare, l'esattezza, intesa anche come non obsolescenza, dei dati su cui si basano gli accertamenti, la disciplina *privacy* ha fornito un ausilio importante alla corretta rappresentazione della capacità contributiva e, conseguentemente, della individuazione preliminare dei profili di rischio fiscali in base ai quali orientare le verifiche. Il rispetto della disciplina di protezione dei dati ha contribuito a mitigare il rischio di errori, tanto più rilevante rispetto all'analisi condotta sempre più spesso con procedure automatizzate.

Queste procedure sono basate anche sulle più avanzate tecnologie informatiche come il *machine learning* e l'intelligenza artificiale, su raccolte di informazioni di natura personale, assimilabili, per dimensione e varietà, ai cosiddetti *big data*.

È bene chiarire sin da ora che il Garante non ha mai ostacolato il processo di digitalizzazione in sé, tanto meno in ambito fiscale, nella consapevolezza del contributo prezioso che le nuove tecnologie possono offrire all'azione di contrasto dell'evasione fiscale, meglio selezionando gli obiettivi del controllo.

Questo anche al fine di garantire, in ultima analisi, quell'equità fiscale sottesa all'idea stessa della progressività delle imposte sancita con lungimiranza dal Costituente. Questa esigenza di innovazione nell'attività fiscale è emersa con particolare nettezza già a partire dal 2011 e oggi essa è indubbiamente più forte, anche in ragione degli obiettivi posti dal PNRR, tra i quali quello relativo alla digitalizzazione dell'attività amministrativa occupa un ruolo di primo piano.

Il processo di digitalizzazione è, tuttavia, di per sé neutro e come tale può determinare, se bene orientato, notevoli innovazioni e miglioramenti in termini di efficacia ed efficienza dell'azione amministrativa, ma può comportare anche note-

voli rischi e disfunzionalità, se non adeguatamente governato.

Nella complessiva azione di *governance* del processo di digitalizzazione, la disciplina di protezione dei dati può svolgere un ruolo importante al fine di garantire i presupposti di sicurezza dei flussi informativi necessari per impedire la permeabilità delle banche dati e i requisiti di esattezza dei dati trattati, indispensabili per evitare rappresentazioni non veritiere della posizione individuale del cittadino.

Da un lato è certamente vero, come sottolinea il direttore Ruffini, che al fine di elaborare i profili di rischio funzionali ai controlli e allo stesso adempimento spontaneo, è necessario per l'Agenzia disporre dei dati a tal fine necessari raccolti in diverse banche dati. Dall'altro lato, però, è necessario non tanto e non soltanto genericamente una maggiore quantità di dati, ma dati migliori, esatti, pertinenti, aggiornati. Lo stesso direttore ha sottolineato, in audizione, come spesso le banche dati cui attinge l'Agenzia abbiano dati eterogenei per struttura e dimensione, soggetti a rapidi cambiamenti e quindi anche a obsolescenza, con il rischio di disallineamento del patrimonio informativo tra un archivio e l'altro.

È evidente, dunque, come tali carenze depotenzino l'efficacia dei controlli fiscali, e della stessa cooperazione internazionale prevista, ad esempio, dalle varie direttive DAC (*Directives Administrative Cooperation*). La soluzione, dunque, non è tanto nell'estensione del patrimonio informativo – anche mediante interconnessione delle basi dati in sé – quanto nella selezione e uniformazione dei dati cui attingere perché siano effettivamente funzionali allo scopo. Le azioni a cui l'Agenzia per l'Italia digitale (AGID) sta dando corso per attuare le disposizioni del codice dell'amministrazione digitale in materia di interoperabilità delle banche dati – su cui il Garante è pienamente coinvolto al fine di assicurare la conformità alla normativa in materia di protezione dei dati personali – potranno certamente dare buoni frutti al riguardo.

Considerazioni in parte analoghe valgono anche per la semplificazione dei pro-

cedimenti in materia fiscale, secondo quel principio dell'*once only* — già sotteso alla legge 7 agosto 1990, n. 241, e allo Statuto del contribuente — nella parte in cui escludono la possibilità di richiedere al contribuente dati già in possesso dell'amministrazione, evitando interazioni superflue. Per essere utilizzabili proficuamente, tali dati devono essere esatti e aggiornati, oltre che — come sancisce la disciplina di protezione dei dati — pertinenti allo scopo perseguito e non eccedenti lo scopo perseguito dall'amministrazione accedente, la quale deve potere attingervi sulla base di una previsione normativa adeguata che legittimi il trattamento del dato per la specifica finalità perseguita.

L'interoperabilità, infatti, come ribadito anche dall'articolo 50 del codice dell'amministrazione digitale, non può essere intesa come indiscriminata possibilità di circolazione per i fini più vari dei dati personali — *a fortiori* se appartenenti alle categorie speciali di cui agli articoli 9 e 10 del GDPR (Regolamento generale sulla protezione dei dati) e cioè gli ex dati sensibili e giudiziari — tra le più diverse amministrazioni, per il solo fatto di essere stati acquisiti *once*, una volta, da uno di esse. Ove così fosse, si determinerebbe l'abrogazione implicita della disciplina di protezione dei dati nella parte in cui impone una previsione normativa puntuale per il trattamento per fini di interesse pubblico o nell'esercizio di pubblici poteri, in violazione dei principi di liceità, correttezza e trasparenza e di limitazione della finalità del trattamento previsti dall'articolo 5 del Regolamento.

Non vanno, peraltro, trascurate le implicazioni in tema di sicurezza, intesa anche come sicurezza nazionale, e non solo nella sua declinazione tecnica informativa, connesse a un modello di interoperabilità — prospettato, come nel caso della Piattaforma digitale nazionale dati di cui all'articolo 50-ter del codice — che include appunto anche le basi dati di rilievo per l'Agenzia. Tutto questo nella forma della centralizzazione e concentrazione di dati anche particolari, riferiti all'intera popolazione, per finalità non adeguatamente cir-

coscritte e con affidamento della gestione a una società, quale PagoPA, i cui compiti rispetto al trattamento non sono sufficientemente individuati.

In assenza di adeguate misure, infatti, la concentrazione in un'unica piattaforma di dati così rilevanti quantitativamente e qualitativamente può accrescerne i rischi di vulnerabilità e costituire di per sé un *target* preferenziale e oltre modo pagante — fosse anche limitatamente alla procurata indisponibilità — di attacchi informatici di vario genere anche eterodiretti. Questo vanificherebbe, oltretutto, i miglioramenti apportati nel tempo alle varie banche dati ora interconnesse, in ottemperanza alle indicazioni del Garante.

In ogni caso l'interoperabilità non è di per sé sola un requisito di efficienza, potendo esserlo, anche in misura significativa, soltanto quando sia assistita da adeguate garanzie di sicurezza e di protezione dei dati che nel caso della piattaforma nazionale dati esigono miglioramenti e anche significativi. Come già osservato, ad esempio, dal Comitato europeo per la protezione dei dati in ordine all'interoperabilità delle App di tracciamento COVID-19, ma con valenza più generale, l'obiettivo dell'interoperabilità non può legittimare di per sé una raccolta di dati personali eccedenti le specifiche finalità di volta in volta perseguite. È significativo che anche il documento conclusivo dell'indagine conoscitiva delle Commissioni finanze congiunte dei due rami riconosca come l'interoperabilità delle banche dati e la digitalizzazione dell'attività fiscale debba avvenire nel rispetto della disciplina *privacy*.

Una reale innovazione e semplificazione dell'attività fiscale, conforme alla disciplina di protezione dei dati, necessita di un piano organico di sviluppo che si articoli su previsioni normative puntuali per circoscrivere con certezza l'ambito di circolazione legittima dei dati, razionalizzandone l'acquisizione. Tale acquisizione deve riguardare soltanto informazioni fiscalmente rilevanti ed evitarne la duplicazione su garanzie di sicurezza adeguate e su stringenti presupposti di accesso soggettivi e oggettivi, per evitare esfiltrazioni indebite dei dati.

Tali esigenze sono state più volte rappresentate dal Garante nell'ambito dell'attività svolta in materia nella ricerca del migliore bilanciamento tra una maggiore efficacia delle verifiche fiscali e la garanzia del diritto alla protezione dei dati personali dei cittadini, rispetto alla prima più sinergica che antagonista. Alcune osservazioni espresse rispetto ai più recenti provvedimenti relativamente alle analisi di rischio fiscale, agli strumenti di determinazione sintetica del reddito necessari ai fini dell'emersione della base imponibile e a quelli volti ad agevolare la *compliance* dei contribuenti (come lo spesometro e la fatturazione elettronica) meritano una riflessione ulteriore in vista degli sviluppi futuri.

In ordine all'elaborazione sperimentale dei profili di rischio fiscale attraverso la rilevazione algoritmica delle incongruenze tra i risparmi e il dichiarato, sulla base dei dati contenuti nell'archivio dei rapporti finanziari, il Garante ha suggerito — in particolare tra il 2017 e il 2019 — alcuni correttivi volti a evitare errate rappresentazioni della capacità contributiva, migliorando dunque — anziché ostacolare — l'efficacia dell'analisi.

Riguardo all'interconnessione delle banche dati — prevista sin dal decreto-legge 6 dicembre 2011, n. 201, per l'elaborazione dei parametri di rischio fiscale in base ai quali orientare le verifiche — in occasione della legge di bilancio 2020 che ha introdotto il requisito della pseudonimizzazione dei dati, sarebbe stato opportuno inserire quelle garanzie specifiche che l'articolo 22, paragrafo 2, lettera *b*), del GDPR prescrive per le decisioni fondate su trattamenti automatizzati normativamente previsti. Tali accorgimenti, lungi dal depotenziare l'efficacia dell'azione di contrasto all'evasione, potrebbero promuoverla, correggendo potenziali errori o distorsioni nel processo decisionale automatizzato. Inoltre, potrebbero conferirle — anche nella percezione dei cittadini — quella più forte legittimazione che una combinazione equa di tecnologia e fattore umano può assicurare all'azione amministrativa, garantendo la massima trasparenza al contribuente al fine di favorire l'adempimento spontaneo

con positiva ricaduta sull'efficacia e sull'efficienza dell'attività di controllo.

Tale esigenza potrebbe essere tenuta in adeguata considerazione anche nell'ambito delle riforme attuative del PNRR, ove il ricorso a tecniche di intelligenza artificiale e analisi avanzata dei dati è previsto tra il 2025 e il 2026 quale componente rilevante per poter aggredire il *tax gap*, ridurre la propensione all'evasione fiscale, favorire l'adempimento degli obblighi.

Un aspetto presente nel piano e da valorizzare sarà quello della conduzione di analisi preliminari su dati previamente anonimizzati, all'esito dunque di un processo che li privi di ogni elemento idoneo a consentire una reidentificazione, sia pure solo indiretta, dell'interessato. Fermo restando che ogni eventuale ricaduta individuale dei trattamenti così effettuati deve essere presidiata da un adeguato apparato di garanzie a tutela dei diritti e delle libertà degli interessati.

Questo vale, *a fortiori*, considerando che la stessa legge di bilancio ha introdotto una specifica esimente fiscale, ovvero una norma che abilita l'amministrazione a limitare per periodi circoscritti l'esercizio dei diritti degli interessati per fini di contrasto e prevenzione dell'evasione fiscale, nonché per esigenze di natura tributaria.

Anche a seguito del recepimento di alcune indicazioni rese dal Garante in sede di audizione, il testo finale della norma reca significativi miglioramenti rispetto a quello iniziale. Ad esempio, è stata correttamente esclusa la rettifica dal novero dei diritti suscettibili di limitazioni, nella consapevolezza dell'utilità dell'esercizio di tale facoltà ai fini della stessa esattezza delle informazioni trattate, quindi della corretta rappresentazione della capacità patrimoniale e, conseguentemente, anche del rischio fiscale dell'interessato. Tuttavia la norma, pur migliorata nel testo, contrae in misura non irrilevante i diritti degli interessati e, quindi, i corrispettivi obblighi del titolare, rafforzando ulteriormente l'esigenza di introdurre garanzie generali, almeno rispetto ai trattamenti fondati su processi decisionali automatizzati.

Anche sotto questo profilo, il documento conclusivo dell'indagine conoscitiva sulla riforma dell'IRPEF (imposta sul reddito delle persone fisiche) votato dalle Commissioni finanze omette di considerare che, rispetto al processo decisionale automatizzato, le garanzie di protezione dei dati non possono essere escluse in radice e rappresentano una significativa tutela, non soltanto per il contribuente ma, appunto, per la stessa correttezza dell'attività fiscale.

Un'ulteriore riflessione meriterebbe la disciplina fatturazione elettronica, il cui ambito è stato significativamente esteso con riferimento alla memorizzazione dei *file* fattura con il decreto-legge 26 ottobre 2019, n. 124, convertito con modifiche dalla legge 19 dicembre 2019, n. 157, e il conseguente provvedimento direttoriale, tanto sotto il profilo della tipologia dei dati raccolti quanto sotto quello dell'ambito e delle modalità di utilizzo degli stessi. Ecco, questo è importante: è stato in particolare previsto l'utilizzo a fini fiscali dei cosiddetti « dati fattura integrati », cioè comprensivi di informazioni di dettaglio inerenti la descrizione del bene ceduto o del servizio prestato cui si riferisce la fattura.

Però molti di questi dati — quali ad esempio quelli contenuti negli allegati delle fatture — non rilevano a fini fiscali e possono, invece, rivelare dati di natura sanitaria o la sottoposizione dell'interessato a procedimenti penali. Si pensi al caso di fatture per prestazioni in ambito forense: separazione giudiziale, divorzio, oltre che penale, o anche specifiche informazioni su merci o servizi acquisiti. Ripeto che sono dati non rilevanti in quanto tali a fini fiscali.

La memorizzazione — a prescindere dall'eventuale utilizzo delle fatture elettroniche nella loro integralità — comporta l'acquisizione massiva di una mole relevantissima dei dati contenuti nei circa due miliardi (ce lo dice il direttore Ruffini) di fatture emesse annualmente. Queste fatture sono inerenti, tra l'altro, ai rapporti tra cedente, cessionario ed eventuali terzi, fidelizzazioni, abitudini e tipologie di consumo, regolarità dei pagamenti, appartenenza dell'utente a particolari categorie.

Tale estensione del novero dei dati trattati dall'amministrazione a informazioni non fiscalmente rilevanti contrasta — come del resto abbiamo osservato sia in sede di audizione e sia di parere sul provvedimento direttoriale — con il principio di proporzionalità e rischia di determinare significative vulnerabilità nelle banche dati fiscali estese e interconnesse in misura tale da divenire assai più difficilmente presidabili.

A seguito del parere del Garante, nel luglio scorso, sul provvedimento direttoriale con il quale si sono sottolineati i profili di incompatibilità del trattamento con la disciplina di protezione dei dati, si è però istituito un tavolo tecnico per l'individuazione delle misure migliori, nonostante i limiti intrinseci della norma sui quali è bene riflettere.

In ogni caso, prima di ipotizzare qualsiasi ampliamento del patrimonio informativo dell'amministrazione finanziaria, il legislatore dovrebbe tenere in considerazione un fatto: in base alla costante giurisprudenza del Consiglio di Stato, le dichiarazioni, le comunicazioni e gli atti acquisiti dall'Agenzia delle entrate contenenti dati reddituali, patrimoniali e finanziari e inseriti nelle banche dati della anagrafe tributaria (ivi compreso l'archivio dei rapporti finanziari) costituiscono documenti amministrativi. Per questo sono, quindi, soggetti all'accesso di cui agli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, da parte di chiunque ne abbia interesse. Ne deriva una potenziale, significativa esposizione della sfera privata, laddove i dati nella disponibilità dell'amministrazione finanziaria non risultino necessari al perseguimento in concreto dell'interesse pubblico sotteso al trattamento, e comunque, ripeto, disponibili alla richiesta di chiunque ne abbia interesse, *ex lege* 7 agosto 1990, n. 241.

Gli interventi del Garante in materia dimostrano come la digitalizzazione dell'attività fiscale — questo è importante — esiga di essere inscritta all'interno di un progetto lungimirante e organico che consideri la protezione dei dati non soltanto come un mero obbligo normativo, ma come un requisito necessario per l'efficacia e l'efficienza delle attività di verifica e *tax com-*

pliance, nonché per rafforzare la fiducia dei cittadini nel ricorso a tecniche di analisi nuove e particolarmente penetranti e pervasive. In questo senso sono da valorizzare in modo particolare i principi di proporzionalità e minimizzazione, circoscrivendo l'ambito del trattamento ai soli dati e alle sole operazioni strettamente indispensabili ai fini perseguiti, adottando misure di *privacy by design* e *by default* che consentono di non interpretare la protezione dei dati come una sorta di *retrofit* da applicare alle grandi banche dati per rendere i trattamenti conformi al regolamento, e favorendo, ove possibile, sempre il ricorso a dati effettivamente anonimi.

Occorre la previsione normativa del trattamento, anche a fronte di nuove ipotesi di interoperabilità dei sistemi, così da evitarne una moltiplicazione incontrollata e ingovernabile, tale da ostacolare anche l'esercizio, abbiamo detto, dei diritti da parte degli interessati, il diritto di rettifica. Occorrono adeguate garanzie rispetto al processo decisionale automatizzato, requisiti di sicurezza e resilienza dei sistemi, essenziali anche a fini di *cybersecurity*.

In conclusione queste misure, a nostro modo di vedere, consentiranno di promuovere una innovazione nell'attività fiscale, tanto da renderla efficace, ma anche rispettosa della *privacy* dei contribuenti, secondo quel bilanciamento tra esigenze collettive e diritti individuali su cui si fondano il nostro sistema ordinamentale interno e quello europeo. Grazie per la vostra attenzione.

PRESIDENTE. Grazie, professore per questo intervento che — credo di poterlo dire a nome della Commissione — ci apre una visione e prospettive veramente interessanti, se non preoccupanti e che credo abbia stimolato sicuramente le riflessioni di tutti i colleghi commissari. Cedo la parola ai colleghi.

ANDREA DE BERTOLDI. Grazie, presidente e naturalmente grazie al professor Stanzone per la precisa e puntuale attività che svolge, come sempre.

Professore, noi di Fratelli d'Italia da tempo siamo molto preoccupati per un

sistema di potenziale utilizzo delle informazioni private che, in tutti i settori, potrebbe sempre più minare quello che è l'obiettivo di avere una società veramente liberale, rispettosa e democratica. Basta raffrontarsi con Paesi come la Cina, dove l'utilizzo dei dati è di fatto oggi la prima arma di repressione nei confronti della libertà dei cittadini. In un regime comunista come quello cinese è coerente la limitazione dei diritti del cittadino per privilegiare i diritti dello Stato o del partito; in una civiltà occidentale e liberale come la nostra questo deve essere una grossa preoccupazione e purtroppo ci stiamo accorgendo che questo pericolo sta crescendo, quindi avrei piacere anche di sentire un suo parere su questo tema.

Abbiamo visto a livello internazionale quanto i *social* — che raccolgono sempre più dati, informazioni dai fini commerciali in avanti — stiano di fatto impadronendosi non solo di dati, ma anche del pensiero delle persone.

Sembrano banalità, ma i *post* — come li chiamano nella vulgata attuale — che non sono coerenti con quel pensiero che si vuole imporre, vengono cancellati, anche se non sono *post* offensivi, se non sono *contra legem*. La libertà di dire, di affermare delle cose viene controllata, questo è il punto. Questi *social* riescono a controllare il pensiero di singolo cittadino, cioè uno dei miliardi di utenti di quel *social* e questo mi preoccupa tantissimo. Alcuni nostri amici, anche anziani, hanno ricordato la battaglia storica di El Alamein e sono stati bannati da *Facebook*. Questo vuol dire che i *social* sono in grado di controllare quello che ciascuno di noi fa e di decidere quello che può dire e quello che non può dire.

Io penso che anche qui il tema della tutela della *privacy* e della libertà del cittadino sia importante e, venendo più nello specifico, vorrei chiederle una cosa. Secondo lei, da un punto di vista anche informatico, per quello che le è dato conoscere, la Società generale d'informatica (SOGEI) che controlla le banche dati e le informazioni quanto investe realmente, non mi interessa ovviamente l'importo numerico, ma lei ritiene che investa sufficiente-

mente nella difesa, innanzitutto, da possibili attacchi informatici? I nostri dati custoditi in quei computer che abbiamo visto a inizio legislatura nei magazzini della SO-GEI, sono realmente difesi da possibili attacchi? Abbiamo un forte investimento nella difesa dei nostri dati? Questa è la prima garanzia che dobbiamo avere.

Un secondo passaggio riguarda qualcosa di cui lei ha parlato nella sua relazione: l'utilizzo pertinente dei dati. Che garanzia abbiamo che il direttore generale, il funzionario, il capo ufficio non utilizzi quei dati per ragioni non pertinenti? Secondo lei gli obblighi e le sanzioni esistenti sono adeguati all'importanza della tutela del cittadino? Il funzionario che utilizza i dati miei o del presidente Parolo per altre ragioni viola semplicemente una norma — e magari può essere richiamato con due righe che non servono a nulla — oppure ci sono delle norme stringenti, ovvero ci dovrebbero essere? Noi gradiremmo avere da lei suggerimenti (noi classe politica, noi legislatori) per creare delle norme più stringenti, più pesanti verso coloro che hanno accesso e, quindi, che possono utilizzare i dati delle banche dati della pubblica amministrazione.

Concludo, per non rubare il tempo ai colleghi, con il tema della fattura elettronica. Anche qui noi abbiamo fatto delle battaglie, mi permetto di dire, un paio di anni fa quando è stata introdotta la fattura elettronica perché non vedevamo — come non vediamo, ahimè — una tutela sull'utilizzo dei dati. Lei lo ha spiegato benissimo: le informazioni che ci sono in una fattura possono comportare la violazione di segreti industriali, perché ovviamente si può capire che cosa compri e come compri, dove compri, a quale prezzo compri. Noi rischiamo che un'azienda sia fotografata, radiografata completamente e che quelle informazioni possano andare magari al suo *competitor* internazionale. Come sappiamo, oggi le guerre non si fanno quasi più, quando contano, con le armi. Si fanno con le armi dove non contano, nelle periferie; a livello di macropotenze le guerre si fanno magari con i virus, speriamo di no, si fanno con gli attacchi informatici.

Il nostro stimato direttore Ruffini — e nella sua ottica lo capisco — chiede continuamente un maggiore utilizzo delle informazioni della fattura fiscale. Però mi chiedo cosa possiamo fare per garantire, invece, la *privacy*, la riservatezza, la tutela dei legittimi diritti che in una civiltà liberale, vivaddio, dobbiamo tutti noi, con le diverse posizioni politiche, sempre strenuamente difendere. Queste sono le informazioni e i pareri che avrei piacere di avere da lei. Grazie ancora, presidente.

MAURO MARIA MARINO (*intervento da remoto*). Grazie, presidente. Tre cose velocissime, perché alle 9.30 purtroppo inizia la discussione in Aula. La prima è un ringraziamento al presidente per una relazione esaustiva e, devo dire, importante che penso ci indurrà a delle ulteriori riflessioni che danno il senso di come il tema trattato sia un tema veramente trasversale che noi dobbiamo utilizzare nelle sue potenzialità in molti settori.

La seconda è una considerazione che faccio a lei, presidente. Alcune delle considerazioni, scusi il gioco di parole, contenute nella relazione ci fanno pensare che sarebbe utile che lei trasmettesse la stessa ai presidenti della VI Commissione Camera e Senato. Il 30 giugno noi abbiamo approvato delle linee di indirizzo sulla riforma fiscale e anche loro dovrebbero essere edotti sugli aspetti evidenziati dal presidente, così come sarebbe necessario trasmettere la relazione al Governo, perché noi sappiamo che le linee di indirizzo devono essere tradotte in un decreto entro il 31 luglio. Penso che il presidente abbia affrontato degli aspetti che in sede di Commissioni effettivamente erano sfuggiti e, quindi, questo dà il senso dell'importanza di quanto è stato detto e della trasversalità dei temi trattati.

La terza cosa, invece, è una domanda velocissima rispetto al fatto se si può ipotizzare di utilizzare i dati personali in relazione ai videogiochi. Noi sappiamo che sono elementi che in relazione al disturbo da gioco d'azzardo (DGA) possono essere gestiti centralmente, tanto è vero che abbiamo anche le *videolottery* controllate da remoto per evitare che ci siano operazioni

fraudolente. Sarebbe molto interessante capire quali sono gli spazi di azione in un settore come quello, sia a fini di indagine ma sia, anche, perché sarebbe un ulteriore arricchimento che potrebbe essere utile.

So che è un tema specifico che esulava dalla discussione della questione. Però ce ne siamo occupati recentemente in VI Commissione Senato e siamo arrivati alla determinazione di creare una Commissione di inchiesta sul gioco d'azzardo e sulle disfunzioni del gioco pubblico. Per questo mi è venuta questa curiosità e colgo l'occasione importante di avere qui il presidente per porgerla. Grazie.

EMILIANO FENU (*intervento da remoto*). Grazie, presidente. Anch'io mi unisco al ringraziamento al professor Stanzione, perché la relazione è molto importante su un tema che sappiamo essere molto attuale. Condivido quanto richiesto dal collega Marino: effettivamente è necessario inviare questa relazione anche ai presidenti delle Commissioni finanze Camera e Senato. Forse era necessario che chiedessimo noi una relazione di questo tipo prima di concludere l'indagine conoscitiva.

Io ho solo due domande. Condivido quanto detto dal professor Stanzione: è assolutamente necessario temperare le esigenze collettive con gli indirizzi individuali, consapevoli del fatto che il processo di digitalizzazione è inarrestabile — sia in ambito privato che in ambito pubblico — e quindi siamo costretti in qualche modo a regolarlo. I tentativi di arginare in parte, mettere delle piccole dighe e fermare, ad esempio, la fatturazione elettronica, per fare un esempio, non servono a niente. Questo è un processo in cui dobbiamo stare dentro e con il supporto e il consiglio degli enti più autorevoli in questo senso dobbiamo pensare a regolarlo.

Condivido anche quanto detto sulla necessità di riscrivere il tutto in un ambito più ampio, temperando questi interessi. Ho due domande, comunque: una trae spunto da quanto detto in Commissione la volta scorsa in audizione dai commercialisti, che hanno individuato nella loro relazione un principio molto importante, quanto finora disatteso, il principio della simme-

tria informativa. Si tratta della parità del diritto di accesso, almeno ai propri dati, da parte del contribuente rispetto a quello che, invece, è il diritto di accesso da parte della pubblica amministrazione.

Quanto detto e anche quanto scritto nella relazione è condivisibile, però è evidente che la pubblica amministrazione — giustamente, da un certo punto di vista — sta creando le condizioni per accedere a qualsiasi tipo di dato riguardante il contribuente: si sta realizzando il famoso *data lake* e questo va regolato.

Lì andranno a confluire, immagino, tutti i dati di natura patrimoniale, reddituale, ma anche della vita privata in qualche modo, ahimè, del contribuente. Se si va verso una situazione di questo tipo che deve essere regolata, non è necessario garantire almeno al primo titolare di quei dati l'accesso a quegli stessi dati di cui è in possesso la pubblica amministrazione e a cui probabilmente attingerà per effettuare gli studi, i processi di accertamento e le attività che sono necessarie? Questa è la prima domanda, se è necessario garantire una simmetria informativa.

Lei ha parlato anche di fatturazione elettronica integrata e, quindi, parlerei anche di corrispettivi integrati, con la necessità — di cui ha parlato anche lei — di anonimizzare in qualche modo i dati. In ogni caso ritiene necessario integrare i dati della fatturazione elettronica e dei corrispettivi telematici legando, ad esempio, la categoria merceologica dell'acquisto al sistema di pagamento, ma con una finalità che va a esclusivo beneficio dei contribuenti? L'idea è quella di legare, su libera scelta e opzione del contribuente, il suo sistema di pagamento alla categoria merceologica di quello che acquista — per esempio il medicinale e, quindi, la tessera sanitaria — in modo da facilitare in qualche modo la vita dichiarativa del contribuente. Lo stesso si ritroverà l'importo della detrazione visibile in un'applicazione sul mobile e rimborsabile saltando tutto l'aspetto burocratico della dichiarazione dei redditi. Le faccio solo queste due domande e rinnovo il ringraziamento.

CARLA CANTONE. Brevemente, perché condivido molte valutazioni e domande che sono state fatte e ringrazio anch'io il presidente, che è stato molto chiaro: d'altra parte avevo letto la relazione con attenzione. Soprattutto in previsione del PNRR lei insiste molto su questo, soprattutto per l'azione di contrasto agli illeciti fiscali. Possiamo immaginare che cosa succederà, che cosa potrebbe succedere – speriamo che questo non avvenga – ma sicuramente avremo di fronte un periodo che ci obbliga a una grande e forte attenzione.

A proposito di protezione, io non volevo intervenire perché ero soddisfatta della relazione che ho letto, poi ho ascoltato l'intervento del senatore di Fratelli d'Italia. Rispetto alla questione dei *social* si tratta di una vergogna per come viene accettata, perché un'azione di contrasto vera e propria non c'è. Io non saprei come fare però, sicuramente, la trovo una cosa di un'inciviltà totale e sono preoccupata di un'altra cosa a proposito della protezione dei dati. Non so se succede anche a voi, ma a molte persone – me compresa – arrivano dei messaggi sul cellulare che sono trappole vere e proprie. Una delle ultime che a me è arrivata e che ho denunciato all'INPS, attraverso la Polizia postale, sta arrivando a molte persone anziane. Io mi reputo diversamente giovane e, quindi, della categoria di chi non ha più venti anni e ne ho molti di più. Ti arrivano messaggi dell'INPS – ma in realtà non è l'INPS – in cui ti dicono di trasmettere i tuoi dati per avere un buono di 1.500 euro per le spese. Ci sta cascando un sacco di gente, è una trappola per avere i tuoi dati e utilizzarli come vogliono e mi fermo perché di trappole ci sono tantissime.

Io non so come fare a fermarle, se parlare con Tim o con le centrali che utilizzano i nostri dati. Lo dico al presidente dell'Autorità garante della protezione dei nostri dati: ne approfitto per dirgli che le protezioni dovrebbero essere un po' più allargate e tante. Noi siamo abituati a utilizzare questi strumenti per il lavoro che facciamo, ma ci sono molte persone anziane oppure ragazzi e ragazzini che ci cascano; senza poi parlare di quello che

avviene tra i ragazzi che seguono – proprio attraverso il cellulare – delle strade che li portano a fare degli atti inconsulti: sappiamo che cosa succede. Non so se sono andata fuori tema, sicuramente sì. Però ho approfittato della sua presenza, presidente, per farle notare che forse occorre aprire una pagina anche su questo argomento. Lo faccia lei, lo faccia qualcun altro: io credo che noi come Commissione dobbiamo provare a ragionare anche su questa idea di protezione.

Capisco che non è un fatto dell'anagrafe tributaria ma, se chiamiamo in audizione chi dovrebbe essere garante della protezione dei dati, a me viene anche da chiedere questo, oltre a ringraziarla per l'ottima informazione per il lavoro che lei fa con molta capacità professionale. Grazie.

PRESIDENTE. Grazie. Non aggiungo altre considerazioni – anche per non sottrarre ulteriore tempo alla replica del presidente dell'Autorità garante dei nostri dati – perché credo che gli interventi dei colleghi siano stati già di per sé sufficientemente stimolanti. Prego, professore.

PASQUALE STANZIONE, *presidente dell'Autorità garante per la protezione dei dati personali*. Grazie. Io rispondo con estremo piacere a domande che non sono soltanto relative all'anagrafe tributaria, ma mi permetto di dire che sono domande di senso. Io farei riferimento a ciò che la settimana scorsa, nella relazione al Parlamento, ho cercato di sottolineare e vale a dire che noi viviamo in un'era, in una società, in una civiltà digitale o, comunque, avviata a un'estrema automatizzazione. Dobbiamo cercare di governarla attraverso il fattore umano, che significa visione antropocentrica del processo di digitalizzazione non soltanto nel momento di definizione della sua origine, ovvero l'algoritmo, ma altresì nei suoi momenti applicativi. Dobbiamo garantire la trasparenza algoritmica. Questo significa anche dotare gli interessati, i destinatari, tutti quanti noi, di strumenti e rimedi per contestare le soluzioni cui l'algoritmo perviene. Dunque occorre inscrivere nel processo il fattore umano: garantendo una *governance* antropocentrica.

Il riferimento che faceva il mio primo interlocutore è indubbiamente vero. Noi ci muoviamo tra due sistemi: citiamo quello della Cina ma dobbiamo citare anche quello degli Stati Uniti. Nel primo l'individuo è assorbito dalla dimensione collettiva e soprattutto dalle esigenze dello Stato; negli Stati Uniti è tutto il contrario, per cui l'individuale ha la primazia e la dimensione solidaristica è recessiva. L'Europa continua, invece, quasi in una terza via, a garantire la persona e i diritti fondamentali, però in una visione solidaristica. Faccio un solo esempio e cito le famose sentenze della Corte di giustizia dell'Unione europea — Schrems I e Schrems II — che hanno reso inefficace il *privacy shield* per i trasferimenti di dati in territori extraeuropei.

Il messaggio è quello di porre particolare attenzione alla circolazione transfrontaliera dei dati, perché in Paesi extraeuropei ad essi non è accordata la medesima tutela che l'Europa garantisce attraverso i pilastri del suo ordinamento: della tutela della persona, della libertà, dei diritti fondamentali e così via.

Questa via, che potremmo definire mediana, è riassunta nel Regolamento europeo 2016/679, il cosiddetto GDPR, che ha cercato di porre alcuni argini — e qui vengo alle domande del primo oratore — ai nuovi poteri privati che sono rappresentati dalle piattaforme. Lei ha ragione quando si chiede come facciamo a difenderci dalle piattaforme multinazionali come *Google*, *Amazon*, *TikTok*, *Apple*, *Microsoft*. Il Regolamento garantisce al cittadino, a ciascuno di noi, una possibilità di tutela significativa. Al Garante, in particolare, è attribuita questa competenza, vale a dire la strenua tutela dei dati personali. È questo l'obiettivo perseguito dal Garante, con i propri provvedimenti e la propria attività. Visto che è stato fatto il riferimento agli anziani e ai minori, cito a questo proposito il provvedimento nei confronti di *TikTok*, relativo alle modalità di verifica dell'età degli utenti minorenni che accedono alla piattaforma.

Questo mi consente di fare un collegamento all'intervento dell'onorevole Cantone, che lambisce l'argomento. Il tema attiene, infatti, alla cultura della *privacy*,

onorevole, vale a dire una sorta di formazione al digitale, specialmente nei confronti della mia generazione, ma forse anche nei confronti dei più piccoli i quali, con l'affidare al *click* i propri dati, non hanno consapevolezza di quale ambito di circolazione essi possano avere. Nella relazione dell'altro giorno ho descritto la congiuntura attuale in termini di algocrazia, quale potere (e finanche abuso di potere) dell'algoritmo. Ciò che noi e tutte le istituzioni repubblicane dobbiamo impegnarci a fare è diffondere quanto più è possibile, a cominciare dai più piccoli, questa consapevolezza mediante un'adeguata formazione digitale che non abbia contenuto solo interdittivo ma, appunto, formativo. Abbiamo ripetuto molto spesso che quando ci viene detto che il servizio prestato è gratuito non è vero: la controprestazione siamo proprio noi, i nostri dati che sono i pezzi, i frammenti della nostra libertà.

Sul piano della sicurezza, come abbiamo sottolineato al Copasir in audizione, più estendiamo l'ambito di raccolta di dati — più ci esponiamo ad attacchi informatici. Il *cloud* nazionale deve garantire, da questo punto di vista, la massima sicurezza e resilienza.

Alla domanda rivolta sul tema della responsabilità, essa concerne anche i profili di *privacy*, pure rispetto al settore dei videogiochi ove si ripropone il bilanciamento tra l'interesse individuale e quello collettivo che era già emerso, pur sotto altre vesti, con la questione dell'accesso documentale nell'ambito della legge n. 241 del 1990, che ha sancito anche in termini simbolico-culturali una nuova declinazione, in chiave paritaria e non subordinata, del rapporto tra pubblica amministrazione e cittadino. Io ringrazio e mi scuso se siamo andati un pochino più avanti con i tempi, so che i vostri lavori non lo consentono.

PRESIDENTE. Grazie, presidente. Ci sarebbe piaciuto sicuramente proseguire su questo tema e approfondire ulteriormente, ma i dati e gli argomenti che sono stati trattati comunque già ci consentono di riflettere in maniera adeguata. Direi di accogliere le richieste dei colleghi, se il pre-

sidente è d'accordo, di trasmettere la sua relazione anche alle Commissioni finanze di Camera e Senato quale elemento utile, anche se purtroppo post conclusione dell'indagine conoscitiva che è stata fatta. Grazie ancora, professore e grazie ai colleghi che hanno partecipato.

La seduta termina alle 9.40.

*Licenziato per la stampa
il 5 agosto 2021*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO



18STC0150310