

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

**RESOCONTO STENOGRAFICO**

**INDAGINE CONOSCITIVA**

17.

**SEDUTA DI MERCOLEDÌ 10 NOVEMBRE 2021**

PRESIDENZA DELLA VICEPRESIDENTE **FELICIA GAUDIANO**

**INDICE**

	PAG.		PAG.
<b>Sulla pubblicità dei lavori:</b>			
Gaudio Felicia, <i>presidente</i> .....	3	Cardellini Valeria, <i>professore associato presso l'Università « Tor Vergata »</i> .....	7
<b>INDAGINE CONOSCITIVA « DIGITALIZZAZIONE E INTEROPERABILITÀ DELLE BANCHE DATI FISCALI »</b>		D'Amore Fabrizio, <i>professore associato presso l'Università « La Sapienza »</i> .....	6
<b>Audizione di docenti universitari esperti di tecnologie dell'informazione e di rappresentanti della società di riscossione di tributi locali ICA Srl:</b>		Fenu Emiliano (M5S) .....	11
Gaudio Felicia, <i>presidente</i> .....	3, 10, 11, 12	Giannoni Oscar, <i>rappresentante legale della società di riscossione di tributi locali ICA Srl</i> .....	10
		Torlone Riccardo, <i>professore ordinario presso l'Università « Roma Tre »</i> .....	3, 12

PAGINA BIANCA

PRESIDENZA DELLA VICEPRESIDENTE  
FELICIA GAUDIANO

**La seduta comincia alle 8.30.**

**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 di docenti universitari esperti di tecnologie dell'informazione e di rappresentanti della società di riscossione di tributi locali ICA Srl.**

PRESIDENTE. L'ordine del giorno reca: l'audizione di docenti universitari degli atenei di Roma esperti di tecnologie dell'informazione, nelle persone di Fabrizio d'Amore, professore associato presso l'Università « La Sapienza », Valeria Cardellini, professore associato presso l'Università « Tor Vergata », e Riccardo Torlone, professore ordinario presso l'Università « Roma Tre »; a seguire, l'audizione del ragionier Oscar Giannoni, nella sua qualità di rappresentante legale di una società di riscossione di tributi locali, la ICA Srl (Imposte comunali affini).

Per ciò che attiene ai docenti universitari, l'audizione è mirata ad acquisire il loro punto di vista tecnico-scientifico sulle strategie di sviluppo avviate dal Governo in tema di digitalizzazione della pubblica amministrazione. Più in particolare mi riferisco: alla costituenda Piattaforma digitale nazionale dati (PDND) che, attraverso l'uso

di apposite interfacce, persegue l'interoperabilità dei sistemi informativi e delle basi di dati della pubblica amministrazione; al tema dei vantaggi e dei potenziali rischi del progetto di migrazione da parte dei numerosi *data center* pubblici privi dei requisiti minimi di sicurezza e di capacità elaborativa verso la nuova infrastruttura *cloud* nazionale.

Quanto alla società ICA Srl, il ragionier Giannoni vorrà delinearci una panoramica sulla qualità dei servizi digitali utilizzati dalle società di riscossione dei tributi a supporto della fiscalità locale, nonché delle relative eventuali criticità.

Cedo la parola, seguendo l'ordine di convocazione, ai docenti universitari. Prego.

RICCARDO TORLONE, *professore ordinario presso l'Università « Roma Tre »*. Gentile presidente, onorevoli membri della Commissione, vi ringrazio innanzitutto per l'invito a questa audizione. Sono professore ordinario presso l'Università « Roma Tre », dove dirigo un laboratorio di ricerca sulle basi di dati e i *big data* del dipartimento di ingegneria del quale sono direttore vicario. Mi occupo da molti anni di vari problemi relativi al trattamento informatico dei dati in tutte le fasi del loro ciclo di vita: raccolta, trasformazione, integrazione, accesso, analisi, estrazione di conoscenza dei dati raccolti.

In accordo con i miei colleghi farò un breve intervento, riportando alcune mie considerazioni sul tema dell'indagine e sulle correlazioni con il progetto del Polo strategico nazionale (PSN), relativo alla migrazione delle banche dati della pubblica amministrazione verso un servizio di *cloud* nazionale, concentrandomi sul tema di mia maggiore competenza, ovvero l'interoperabilità dei dati in questo contesto e sul problema connesso della loro fruibilità.

I miei colleghi approfondiranno i temi del *cloud computing* e della sicurezza in questo ambito. Premetto che potrò fare soltanto alcune considerazioni generali su questo argomento, non conoscendo nel dettaglio il dominio di interesse, ovvero la quantità, la qualità, la dislocazione geografica e, soprattutto, il livello di eterogeneità delle banche dati fiscali attualmente esistenti, sebbene sia al corrente che abbiamo davanti un panorama molto articolato, con una presenza di più di 150 banche dati. Da tecnico, cercherò inoltre di adottare un linguaggio scevro da tecnicismi troppo spinti per rendere fruibili le mie considerazioni a un'ampia platea.

Vorrei innanzitutto chiarire che, tecnicamente parlando, la prospettata migrazione delle banche dati e dei servizi della pubblica amministrazione nel *cloud* nazionale — il Ministro Colao l'ha previsto entro il 2025 — non risolverà il problema della loro interoperabilità. Il *cloud*, infatti, rappresenta solo una tecnologia che consente di offrire un'infrastruttura ovvero, per dirla in termini semplici, una casa comune sicura e protetta ai dati — della sicurezza parleranno i miei colleghi, sono più esperti — garantendo sovranità nazionale e autonomia tecnologica. Viceversa, l'interoperabilità delle basi di dati è un problema di carattere metodologico che investe un processo teso a garantire l'interscambio e la condivisione di dati tipicamente eterogenei memorizzati su sistemi diversi, tra i quali una possibile scelta, ma certamente non l'unica, è il *cloud*.

Si tratta di un problema con il quale, tipicamente, imprese e istituzioni hanno sempre avuto a che fare da ben prima dell'avvento delle risorse di *cloud*, ed è un problema molto studiato anche nel mondo scientifico. In questo contesto la disponibilità di una risorsa di *cloud* pubblico, nella quale le banche dati della pubblica amministrazione potranno alloggiare nel prossimo futuro, rappresenta certamente un mezzo facilitatore, in quanto offre un'infrastruttura comune ai dati, ma non direttamente per la soluzione del problema. Adottando un linguaggio comune, se due basi dati non si parlano su infrastrutture tra-

dizionali, continueranno a non parlarsi nel *cloud*. A mio parere, quindi, la vera sfida della strategia *cloud* per la pubblica amministrazione è rappresentata proprio dell'interoperabilità, ovvero dalla capacità di fare finalmente dialogare i dati della PA una volta che avranno una casa comune.

Con riferimento al tema dell'adozione di politiche intesa a garantire la interoperabilità delle basi di dati, vedo con pieno favore l'iniziativa attualmente in corso relativa allo sviluppo di un modello di interoperabilità unificato e di una Piattaforma digitale nazionale dei dati. Come sapete, sono coinvolte principalmente l'AgID (Agenzia per l'Italia digitale) e PagoPA Spa in queste iniziative.

Il modello di interoperabilità serve a definire in termini tecnici precisi un meccanismo di cooperazione standardizzata tra le pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche condivise che assicurano l'interazione e lo scambio dei dati senza vincoli sulle implementazioni. Alla base c'è un principio, secondo il quale ogni servizio *software* — per esempio il reperimento dei dati da una specifica banca dati — viene condiviso attraverso un'interfaccia digitale pubblica chiamata *Application programming interface* (API), che è basata su standard condivisi e garantisce accesso controllato al servizio. Questa soluzione ha una serie di vantaggi: favorisce lo sviluppo di nuove applicazioni al servizio del cittadino, assicura l'accesso ai dati della pubblica amministrazione anche a soggetti terzi ed è coerente con principi definiti anche a livello europeo.

Viceversa, la Piattaforma digitale nazionale dei dati per l'interoperabilità — come voi sapete, si è appena conclusa una consultazione pubblica di un primo documento descrittivo di questa piattaforma — è uno spazio virtuale atto ad agevolare le amministrazioni nell'adozione di questo modello di interoperabilità, nel quale ciascun ente potrà rendere disponibili le proprie informazioni secondo regole condivise, basate su questo meccanismo delle API. Più specificatamente, questa Piattaforma nazionale dei dati è costituita: da un catalogo

delle API prodotte dalla pubblica amministrazione, che la piattaforma rende disponibile ai soggetti accreditati, da meccanismi per l'accreditamento, l'identificazione e la gestione di livelli di autorizzazione e da strumenti per la raccolta e la conservazione delle informazioni relative agli accessi e alle transazioni effettuate tramite questa piattaforma.

Va osservato che in base al decreto legislativo sul Codice dell'amministrazione digitale, in prima applicazione la piattaforma dovrebbe assicurare prioritariamente, con questo sistema, l'interoperabilità con le basi di dati di interesse nazionale – che includono, per esempio, l'Anagrafe nazionale della popolazione residente e il registro delle imprese – con le banche dell'Agenzia delle entrate individuate dal suo direttore. Ne consegue che gli enti che gestiscono le banche dati fiscali dovranno attrezzarsi in breve tempo per essere in grado di generare queste API per l'accesso ai dati, secondo le linee guide definite dall'AgID.

In questo quadro ci sono due importanti considerazioni da fare. La prima considerazione è che i progetti relativi al *cloud* nazionale e alla Piattaforma digitale nazionale dati sono pienamente coerenti. Infatti il meccanismo di accesso alle informazioni basate sulle API adottato dalla Piattaforma nazionale dati è di tipo *black box*, ovvero ne nasconde i dettagli implementativi, inclusa la specifica tecnologia utilizzata per la memorizzazione dei dati. Ne consegue che è tecnicamente possibile sia modificare l'applicazione *software* che opera sui dati, sia migrare i dati da una piattaforma a un'altra senza che le API, queste interfacce digitali, vengano modificate, purché sia garantita la consistenza del suo comportamento, quindi senza che gli utilizzatori ne abbiano contezza. La migrazione nella Piattaforma digitale dati avrà un impatto relativamente basso sul processo di adozione di questo modello di interoperabilità.

La seconda considerazione è che il modello di interoperabilità unificato e la Piattaforma nazionale dati non costituiscono ancora la soluzione definitiva al problema dell'interscambio di informazioni tra le ban-

che dati della PA. Definiscono uno strumento tecnologico fondamentale, basato su standard condivisi, ma sarà necessario sviluppare nuove applicazioni che, utilizzando questo strumento, siano in grado di comporre le funzionalità offerte dalle API disponibili nella Piattaforma nazionale dati, al fine di offrire una soluzione in grado di combinare i dati memorizzati in basi dati di amministrazioni diverse o in basi dati diverse della stessa amministrazione. Per ottenere questo è importante un ulteriore ingrediente: fare uso nella produzione di queste API di un vocabolario comune o, per dirla in termini più tecnici, di un'ontologia condivisa o una collezione di ontologie specializzate per i vari domini applicativi. In termini semplici, un'ontologia serve a capire che due termini diversi utilizzati in due banche dati rappresentano lo stesso concetto e a descrivere l'esistenza di una correlazione semantica tra termini che rappresentano concetti diversi. Questo aspetto è citato nelle linee che definiscono il modello di interoperabilità, nelle quali si invitano le amministrazioni ad aderire, nella produzione delle API, a una collezione di ontologie di dominio che l'AgID sta raccogliendo, ma è di fondamentale importanza – questo lo vorrei sottolineare – per il raggiungimento di una piena interoperabilità tra le banche dati della pubblica amministrazione.

L'ultima considerazione che vorrei fare è legata al problema della fruizione dei dati da parte dei cittadini in questo contesto. Deve essere chiaro che il meccanismo delle API a supporto dell'interoperabilità non è pensato per essere utilizzato direttamente dall'utente finale, cioè dal cittadino, ma favorisce il dialogo tra i componenti *software*, quindi nasce per offrire un supporto ai programmatori nello sviluppo delle applicazioni. Una volta che queste operazioni andranno in porto, sarà necessario un ulteriore sforzo da parte delle istituzioni – anche da soggetti terzi, perché questo è consentito dalla piattaforma – atto a garantire lo sviluppo di applicazioni al servizio del cittadino che, facendo leva sul modello e l'infrastruttura tecnologica che è stata realizzata, sia in grado di semplificare

l'accesso ai servizi della pubblica amministrazione attraverso un meccanismo con accesso unificato e di facile uso.

Chiudo il mio intervento osservando che un contributo importante a tutte le attività di cui ho parlato può essere fornito dai centri di ricerca pubblici, in particolare dalle università lungo due direzioni. La prima, ovviamente, è quella della formazione. Uno degli ostacoli maggiori al processo che ho delineato è la scarsità di competenze tecniche e in questo le università giocano un ruolo fondamentale, essendo loro compito istituzionale quello di formare professionisti capaci di affrontare le sfide che abbiamo davanti. L'altra riguarda il contributo che docenti e ricercatori delle università possono offrire in termini di metodi e strumenti innovativi che sono il risultato della loro attività di ricerca, attraverso quel tanto auspicato trasferimento di conoscenze che le università possono fornire alle istituzioni e alle imprese di questo Paese. Vi ringrazio per l'attenzione e sono a disposizione per eventuali domande e chiarimenti.

FABRIZIO D'AMORE, *professore associato presso l'Università « La Sapienza »*. Grazie. Egregi onorevoli, rispettati colleghi, porgo i miei saluti. Desidero ringraziare la Commissione per questa opportunità. Sono docente in « Sapienza » dall'inizio degli anni Novanta e mi sono sempre occupato di informatica teorica e algoritmica. Da circa dieci anni mi occupo di sicurezza e *privacy*.

È dai tempi delle famose leggi Bassanini che sento parlare di digitalizzazione, semplificazione e firma digitale. Tuttavia, quello a cui ho potuto assistere non era esattamente in linea con le tematiche menzionate. Tutto diveniva continuamente più complesso, burocratico, nella cultura del sospetto e la penetrazione della firma digitale piuttosto scarsa. Gli accademici che studiano la *cybersecurity* sono spesso impegnati sul fronte della ricerca che si posiziona su temi estremamente specialistici.

La digitalizzazione, nonché l'associata sicurezza, sono temi già noti da almeno un ventennio che, per un motivo o per l'altro, sono stati applicati e sviluppati maldestramente. È mia opinione che esistano poten-

zialità ancora smisurate, legate a una digitalizzazione applicata correttamente e un insieme di operatori non impreparato ad essa. In altre parole, vedo un importante efficientamento della pubblica amministrazione, di cui si sono potuti intravedere piccoli esempi a causa della pandemia, ovvero di un'importante motivazione; quasi forse che l'efficientamento della pubblica amministrazione non fosse un'importante motivazione. E che tutto avvenga all'insegna della sicurezza permette di assicurare velocità, ridurre errori e costi.

Da ciò derivano due temi fondamentali ugualmente validi nel mondo pubblico e privato: la dirigenza deve governare l'informatica e definire politiche di *governance* in maniera corretta e oculata, legate alle finalità per cui i processi sono destinati; gli operatori debbono usare consapevolmente gli strumenti informatici nel rispetto delle politiche assegnate.

In generale, appare irrinunciabile non gestire la sicurezza e la *privacy* attraverso un approccio strutturato e corretto. È nota l'esistenza di due famiglie di attacchi informatici: quelli a pioggia, per il solo fatto di essere raggiungibili da *Internet*, e quelli mirati, in cui il bersaglio è unico e precisamente individuato.

Semplificando, ci si difende abbastanza bene dai primi con una corretta igiene della sicurezza che richiede, quindi, formazione. Mentre i secondi sono efficaci e micidiali. Credo che potrebbe esserci una svolta in termini di efficientamento anche solo preparandosi ai primi, mentre è assai impegnativo difendersi dai secondi, e si può decidere di farlo solo in casi molto importanti, se non critici.

Non sono favorevole a regole stringenti e severe sull'uso delle *password*. A mio avviso, oltre a favorire comportamenti insicuri, si osserva un danno economico associato al tempo necessario a ritrovare una *password* o rigenerarla. Tale danno andrebbe sommato per tutti i casi che si verificano in un periodo, danno superiore ai benefici ottenuti dall'incremento di sicurezza delle *password* nello stesso periodo. Il tema può essere sviluppato nell'ambito dell'igiene della sicurezza.



Sono favorevole alla sicurezza e alla *privacy by design*, piuttosto che *by patching* per ragioni di flessibilità, scalabilità e applicabilità, senza perdere di vista i vantaggi economici. Per le stesse ragioni tali obiettivi dovrebbero essere raggiunti attraverso un approccio il più possibile aperto: non è un caso che il più usato metodo di cifratura dell'informazione — ancora sicuro — sia stato promosso dall'americano NIST: il *National institute of standards and technology* propose l'*Advanced encryption standard* (AES), come metodo standard di cifratura dell'informazione nel 2001. Propose questo metodo in modalità *open source*, per cui una comunità mondiale di dimensioni ragguardevoli l'ha testata e studiata per oltre un ventennio, potendo ottenere la consapevolezza che la sicurezza del metodo deriva dalla sola segretezza della chiave. Ciò in opposizione alla *security by obscurity*, assai più onerosa, vista la platea ridotta di *tester* e il fatto che ci si trovi a dover modificare continuamente parametri e chiavi.

Tale argomento non è irrilevante, trova immediatamente applicazione nell'odierna discussione relativa al *cloud* per la pubblica amministrazione. Una proposta emersa da soggetti autorevoli ha menzionato l'uso di un metodo di cifratura nazionale, ma si può replicare con due osservazioni: per raggiungere il livello di sicurezza pari a quello che oggi si può avere già disponibile e *open source* occorrono anni, se non decenni; lo standard oggi disponibile, trascurando vari altri esempi di qualità, è l'AES proposta dal NIST, che è stato testato e attaccato da venti anni ed è noto per la sua robustezza.

Ciò posto, appare irragionevole la proposta di un metodo di cifratura nazionale per i suoi tempi e per le risorse necessarie, pur disponendo di ottimi crittografi sul territorio nazionale. Appare più promettente lo studio/analisi di come applicare i requisiti della sicurezza delle informazioni — i cosiddetti requisiti CIA (Confidenzialità, Integrità, Disponibilità) — oltre a non ripudio, autenticazione, *accounting*, ai dati trattati. Quali categorie di informazione ne sono interessate e come farlo? È un que-

sito a cui si risponde dando un giusto riscontro al tema precedente, relativo alla *governance* della sicurezza. Sottovalutare ciò conduce a disastri annunciati.

Una volta identificati alcuni dati da cifrare, quali soluzioni pratiche occorre adottare? Questa è una questione tecnica, non è sufficiente scegliere un buon metodo, bisogna domandarsi se la cifratura vada fatta a livello di *file system*, di DBMS (*Database Management System*) o a livello utente. Appare cruciale la politica di gestione della chiave, unica informazione che necessita di essere mantenuta segreta. Piuttosto che discutere di quali *cloud* italiani, europei, extraeuropei convenga utilizzare, occorre individuare servizi *cloud* di adeguato livello certificato, in cui la gestione delle chiavi di cifratura venga lasciata all'utente, così che l'intervento di uno Stato straniero che cerchi di violare i dati risulti vano e la gestione delle normali operazioni di ricerca testo vengano fatti attraverso la cosiddetta crittografia omomorfa. L'unica ragione per cui appare preferibile l'uso di un *cloud* nazionale o europeo è il requisito di disponibilità dei dati, il terzo dei requisiti CIA. Questo onde prevenire la possibilità che uno Stato straniero possa bloccare l'accesso ai dati rendendoli inarrivabili.

L'altra questione, relativa all'uso consapevole degli strumenti informatici da parte degli operatori, è legata alla disomogeneità e alla scarsità della cultura di base informatica, inclusa un'alfabetizzazione sulla sicurezza. Limiti che occorre superare in maniera netta e totale, facendo dimenticare il passato a costo di dover affrontare possibili crisi sindacali. La formazione — differente da quella necessaria per la *governance* dell'informatica — appare l'unico strumento viabile, non affidandolo a casaccio ma a persone che, più che depositarie di competenza tecnica, siano didatticamente esperte e valide, perché gli argomenti in questione sono disciplinarmente di base, piuttosto che avanzati. Grazie a tutti.

VALERIA CARDELLINI, *professore associato presso l'Università «Tor Vergata»*. Gentile presidente, onorevoli membri della Commissione, vi ringrazio per avermi invi-

tato a questa audizione. Sono professore associato presso l'università di Roma « Tor Vergata », dove svolgo attività di ricerca e di didattica sui sistemi e servizi in ambito *cloud* e *big data* all'interno del dipartimento di ingegneria civile e ingegneria informatica. Da oltre venti anni mi occupo di sistemi *software* distribuiti, dedicando una particolare attenzione ai sistemi e servizi basati sul paradigma del *cloud computing* e sulle sue evoluzioni più recenti su cui lavoro da più di dieci anni. In accordo con i miei colleghi presenti, il professor D'Amore e il professor Torlone, nelle mie considerazioni sull'argomento dell'indagine conoscitiva porrò l'attenzione sul *cloud computing*, che è il tema di mia maggiore competenza tra quelli di interesse per l'audizione odierna. Dal momento che non conosco in dettaglio le caratteristiche tecniche dei dati e dei servizi delle infrastrutture e delle piattaforme dell'amministrazione finanziaria centrale e di quelle locali, nel mio intervento presenterò alcune considerazioni sull'argomento di carattere generale.

Il *cloud computing* è un paradigma di erogazione di servizi offerti a livello di infrastrutture, piattaforme e servizi da fornitori detti *cloud service provider*, attraverso la rete *Internet* e rappresenta il maggior abilitatore tecnologico della trasformazione digitale e dei principali *trend* tecnologici innovativi come l'*Internet of things* (IoT), l'analisi dei *big data*, l'intelligenza artificiale e il *quantum computing*. Il paradigma del *quantum computing* non è un paradigma nuovo, in quanto inizialmente i primi servizi li abbiamo avuti nel 2006, ma l'idea del *cloud computing* come *public utility* risale addirittura al 1961, e nell'informatica 60 anni sono un'era geologica.

Nel corso di questi quasi due anni di pandemia di COVID-19, il *cloud* si è rivelato, dal punto di vista tecnologico, un ottimo alleato per rispondere in modo efficace e rapido alla situazione di enorme fragilità in cui ci siamo trovati. In base ai dati dell'osservatorio *cloud transformation* del Politecnico di Milano, nel corso del 2020 in Italia vi è stata una crescita di adozione del *cloud* e migrazione verso di

esso del 21 per cento rispetto al 2019 e in particolare l'adozione è arrivata al 42 per cento nelle piccole e medie imprese.

Nel corso del 2021 la crescita già registrata nel 2020 è continuata, con stime che indicano una crescita complessiva della spesa del 16 per cento. Il 44 per cento delle applicazioni delle grandi aziende è ormai gestito usando i modelli di distribuzione o del *deployment* dei servizi *cloud* denominati *cloud* pubblico e privato. Nel primo caso, *cloud* pubblico, l'infrastruttura IT (*Information technology*) è di proprietà del *service provider* che eroga servizi disponibili al pubblico attraverso *Internet*, su risorse condivise da molteplici utenti. Nel secondo caso, il *cloud* privato, l'infrastruttura è dedicata esclusivamente all'organizzazione che ne ha il pieno controllo. Inoltre i modelli di *deployment*, denominati *cloud* ibrido e *multicloud*, sono in rapido corso di adozione a livello internazionale. Il primo rappresenta una combinazione del modello pubblico e di quello privato, mentre il secondo modello prevede l'utilizzo contemporaneo di più *cloud* dello stesso tipo, pubblico o privato, offerti però da diversi fornitori.

Come indicato nel documento « Strategia *cloud* Italia », la scelta del modello di distribuzione *cloud* da utilizzare è strettamente collegata al tema della sovranità dei dati. Pertanto in tale documento è stato indicato correttamente, come approccio di selezione del modello di distribuzione, quello orientato alla criticità dei dati e dei servizi. In particolare è stata indicata la necessità di utilizzare per i dati di servizi critici – ovvero quei dati che, se compromessi, potrebbero pregiudicare la continuità di funzioni della pubblica amministrazione rilevanti per la società, la salute e la sicurezza – i modelli di *cloud* pubblico criptato, privato ibrido su licenza e privato qualificato. I dati e i servizi strategici invece – ovvero quei dati che hanno un impatto diretto sulla sicurezza nazionale – potranno usufruire soltanto dei modelli privato ibrido su licenza e privato qualificato.

I benefici del *cloud* in termini di riduzione dei costi da una parte e miglioramento di prestazioni, sicurezza, resilienza,



continuità di servizio e sostenibilità energetica devono necessariamente essere colti e sfruttati a pieno per l'erogazione dei servizi della pubblica amministrazione. Infatti, tra i principi guida enunciati nel Piano triennale per l'informatica della pubblica amministrazione 2020/2022 è presente il principio del *cloud* come prima opzione, ovvero le pubbliche amministrazioni, nella definizione e sviluppo di nuovi servizi, dovranno adottare in modo primario il paradigma *cloud*. Tale principio è stato ribadito come pilastro del progetto di digitalizzazione della PA enunciato nel PNRR (Piano nazionale di ripresa e resilienza) italiano.

Pertanto, viene auspicato anche nel documento « Strategia *cloud* Italia » che i servizi erogati siano basati su applicazioni cosiddette *cloud native*, ovvero applicazioni sviluppate nativamente sulla base dei paradigmi del *cloud computing*. A questo proposito, come mia prima considerazione, vorrei evidenziare come nella migrazione verso il *cloud* — che rappresenta un'attività complessa, in quanto coinvolge non soltanto aspetti tecnologici, ma anche culturali e di processo — rivesta un ruolo cruciale non soltanto la migrazione dei dati, ma anche la migrazione dei servizi utilizzati per accedere ai dati, per memorizzarli, processarli e analizzarli ai fini di estrarne valore aggiunto. Pertanto è fondamentale che i servizi siano opportunamente riprogettati per usufruire a pieno dei benefici del *cloud*, ad esempio utilizzando soluzioni tecnologiche moderne come le architetture a microservizi. I microservizi, basandosi su un'architettura distribuita e sfruttando le tecnologie di virtualizzazione leggera, permettono in particolare di ottenere una maggiore flessibilità e resilienza, una gestione dei dati decentralizzata (e questo vuol dire l'utilizzo di diverse banche dati anche specifiche e dedicate per singolo microservizio) e una continua scalabilità delle applicazioni così sviluppate. Nel processo di migrazione dei dati e dei servizi risulta importante l'identificazione dei servizi che saranno migrati nel *cloud*, seguendo un approccio incrementale e iterativo.

Inoltre, richiamandomi ai modelli di distribuzione del *cloud* che ho prima bre-

vemente descritto, ritengo sia importante fornire all'amministrazione centrale e alle amministrazioni locali delle linee guida chiare e di facile adozione che consentano di identificare agevolmente il modello di distribuzione più appropriato. Non soltanto con riferimento alla classificazione della criticità dei dati, ma anche dei servizi. Ad esempio, ricordiamo il caso del rilascio — quasi un anno fa — dell'applicazione del *cashback* di Stato e dei servizi che gli utenti hanno sperimentato nei primi giorni di utilizzo. Questo a causa della mancata scalabilità di alcune componenti del servizio, che ha impedito di sfruttare uno dei vantaggi principali del *cloud*, ovvero l'elasticità.

Con il termine « elasticità » si intende che la capacità di effettuare computazioni e memorizzazione dei dati possa essere dinamicamente ottenuta e rilasciata in modo autonomo, ovvero richiedendo un intervento umano al più minimale per scaricare rapidamente e in modo commisurato alla domanda di servizio. In questo modo, per l'utente dei servizi *cloud* la capacità disponibile appare spesso illimitata e il sistema adegua dinamicamente l'utilizzo delle risorse rispetto alla domanda, sia in quantità che nel tempo, riducendo così i costi e l'inefficienza energetica causata dal sovradimensionamento dell'infrastruttura di servizio. L'elasticità permette di affrontare serenamente quell'incertezza insita nell'utilizzo dei servizi, non soltanto servizi *cloud*, dovuta, ad esempio, a variazioni improvvise e a volte imprevedibili nella domanda di servizio.

Come seconda osservazione vorrei richiamare l'attenzione sulla necessità di avere un'infrastruttura — in particolare offerta da quelli che saranno i fornitori del *cloud* privato ibrido su licenza e privato qualificato che saranno selezionati — che sia in grado di supportare adeguatamente questa importante caratteristica del *cloud*, insieme agli aspetti di disponibilità, affidabilità e resilienza a malfunzionamenti, non soltanto derivanti da attacchi di *cybersecurity*. Ad esempio, ricordiamo un mese fa un importante disservizio a livello mondiale che ha colpito alcune applicazioni di uso

comune, che è stato legato a un errore di configurazione da parte degli operatori dell'infrastruttura.

Vorrei infine sottolineare l'importanza della standardizzazione, dell'armonizzazione e dell'interoperabilità dei servizi *cloud* offerti da diversi fornitori, in particolare ai fini di evitare il rischio del cosiddetto *vendor lock-in*. Questi sono aspetti che presentano ancora alcuni elementi di criticità che sono oggetto di dibattito anche nella comunità scientifica internazionale.

Infine, concludendo il mio intervento e come anche evidenziato dai colleghi, vorrei sottolineare il contributo importante che può essere fornito dai centri di ricerca pubblici, in particolare dalle università, nella direzione del trasferimento di conoscenza delle attività di ricerca in cui siamo coinvolti ogni giorno e nella direzione della formazione. In particolare delle giovani donne, auspicando una maggiore parità di genere che nell'ambito informatico presenta, in particolare, un divario significativo. Vi ringrazio per l'attenzione.

**PRESIDENTE.** La ringrazio e restiamo in attesa della relazione. Procediamo con il ragioniere Oscar Giannoni. Prego.

**OSCAR GIANNONI, rappresentante legale della società di riscossione di tributi locali ICA Srl.** Buongiorno a tutti. Vorrei ringraziare il presidente e la vicepresidente della Commissione per l'onore di averci convocato per questa audizione.

La società che rappresento è una società che opera nel settore della riscossione dei tributi locali delle entrate patrimoniali da oltre 60 anni ed è iscritta all'albo dei concessionari di cui all'articolo 63 del decreto legislativo n. 446 del 1997. La nostra interfaccia pubblica è l'Agenzia delle entrate riscossione. Lavoriamo esclusivamente per gli enti locali: comuni e province in particolare ed enti a questi collegati. Il nostro scopo principale è di dare ai comuni e ai cittadini contribuenti un servizio efficiente ed efficace. Per ottenere questo naturalmente è necessario avere accesso a banche dati aggiornate e puntuali, purtroppo — sintetizzo un po' la relazione — a oggi,

nonostante si siano succeduti negli anni vari atti normativi che ci consentivano questo accesso, per una serie di motivi non imputabili ai concessionari e, forse, neanche ai gestori di queste banche dati, non siamo mai riusciti ad avere un pieno accesso alle banche dati stesse.

Nella legge di bilancio 2020 c'è stato un passo significativo, nel senso che è stato concesso agli enti locali di consentire, sotto la propria responsabilità, l'accesso alle occorrenti banche dati anche ai concessionari della riscossione e dell'accertamento. Tutto questo però ha una criticità fondamentale che è legata al fatto che, lavorando anche come azienda con oltre mille comuni di varie dimensioni — dai comuni più grandi, capoluoghi di provincia, di regione, a comuni effettivamente molto piccoli di poche centinaia di abitanti — le differenze sono notevoli.

Le banche dati e i sistemi Sister concessi, che sono le principali banche dati dell'Anagrafe tributaria, hanno dei limiti nei confronti degli enti più grandi in termini di numero di accessi, per cui gli accessi consentiti ai concessionari sono comunque limitati, a volte quasi inesistenti, perché vengono utilizzati direttamente dai dipendenti pubblici. I comuni più piccoli hanno un problema più di conoscenza. Tale criticità potrebbe essere risolta con un'autorizzazione diretta ai concessionari all'accesso alle banche dati. Quindi, visto che siamo iscritti a un albo gestito dal Ministero dell'economia e delle finanze e, comunque, sotto il controllo dello stesso, potremmo essere autorizzati ad accedere direttamente, così come ad altri livelli l'Agenzia delle entrate riscossione può fare con i suoi dipendenti.

Le banche dati a cui attualmente possiamo accedere sono: Telemaco, InfoCamere, Copernico, Sister, INI-PEC, Siatel, l'Anagrafe nazionale della popolazione residente e quelle dell'INPS (Istituto nazionale della previdenza sociale). Sono tutte banche dati utilissime per le notifiche degli atti che devono essere puntuali, per non creare disservizi agli enti e ai cittadini. Alcune di queste banche dati, tuttavia, sono a pagamento, il che comporta un danno

per il concessionario che, a sua volta, ha un suo conto economico e deve ribaltare quest'onere sui cittadini o sugli enti. Quindi sarebbe opportuno che l'accesso a queste banche, essendo realizzati per un fine pubblico, avessero una gratuità di fruizione.

Peraltro gli stessi servizi delle banche dati, anche nei confronti degli enti locali, a volte sono a pagamento, non tutti sono gratuiti. Quindi non è solamente un problema di concessionari, ma proprio di enti locali. Questo potrebbe essere consentito anche mediante la fruizione di modelli standard omogenei. Per l'Anagrafe tributaria penso all'ANCI (Associazione nazionale comuni italiani), con riguardo all'interrogazione anagrafica con elenchi (il PFC 115 come termine tecnico) o l'anagrafica delle persone fisiche con elenchi domiciliari, i domicili fiscali. Anche delle altre banche dati si potrebbe fruire con le stesse modalità di sicurezza disponibili. Naturalmente nessun dato deve potere essere scaricato dal concessionario, così come non lo è dal comune, per creare una propria banca dati, ma solo per atti strettamente necessari. Questo potrebbe avvenire con l'identificazione dell'atto direttamente all'acquisizione del dato.

Altrettanto importante è sottolineare l'accesso massivo dell'acquisizione dei dati che ha un duplice scopo, di accelerare le modalità di acquisizione dei dati di lavorazione degli atti e di evitare operazioni manuali di operatori che, comunque, limitano anche accessi fraudolenti sulle banche dati.

Tra le ultime cose che sono importanti per noi concessionari sono le posizioni patrimoniali e reddituali dei contribuenti, che a oggi sono molto limitate, essendo legate solamente alla dichiarazione dei redditi e al sistema Sister, quindi ai dati catastali. Altrettanto importante — anzi, direi essenziale — è l'accesso alle banche dati finanziarie, non tanto sugli importi, che sono legati a un particolare momento, ma l'istituto di credito o l'ente finanziario aggredibile. Questo per poter finalizzare meglio il pignoramento presso terzi che oggi, in mancanza di questi dati, principalmente è legato ai dati che si rilevano dall'INPS e dagli uffici del lavoro, quindi di pignoramento di

stipendi e pensioni. Altri beni aggredibili, in particolare per le società e i soggetti titolari di partita IVA, potrebbero essere altrettanto importanti. Mi limiterei a questo.

**PRESIDENTE.** La ringrazio. Chiedo ai colleghi se ci sono domande, è collegato il collega Fenu che ne ha. Prego, collega Fenu.

**EMILIANO FENU.** Ringrazio innanzitutto gli auditi per le spiegazioni molto tecniche, molto interessanti che ci hanno fornito. Credo sia fondamentale l'alfabetizzazione, diciamo che stiamo procedendo un po' tutti da autodidatti in questo senso e ci stiamo destreggiando nelle tecnologie. Questi discorsi forse non vanno resi pubblici, in realtà, ma questo è stato detto da alcuni auditi, bisogna tendere alla maggiore semplicità possibile per quanto riguarda l'aspetto della fruibilità, sia da parte dell'utente privato, che anche da parte dell'utente pubblico. Perché, ovviamente, l'utilizzo di queste banche dati e anche le procedure di sicurezza devono essere rese nella forma più semplice possibile, esattamente come fanno quelle che conosciamo e le cui applicazioni utilizziamo ogni giorno. Sono sicuramente molto efficienti e, allo stesso tempo, di facile utilizzo.

La mia domanda è questa, la chiedo innanzitutto agli accademici e un po' esula da quello che ci hanno spiegato sui *cloud*, tutte cose assolutamente interessanti che già utilizziamo nella vita privata. Volevo chiedere se ci sono nel mondo accademico, nelle università, dei sistemi, delle occasioni di coinvolgimento delle giovanissime generazioni. Perché noi semplici cittadini che non svolgiamo il mestiere di accademico, di tecnico, di studioso della tecnologia ci stiamo destreggiando. Sicuramente chi insegna è assolutamente preparato e studia queste cose da anni, ci hanno spiegato anche in che termini. Però chi può fare qualcosa di innovativo sono le giovanissime generazioni. La metafora, il paragone che ho in testa è: l'uomo può essere bravissimo, il migliore del mondo a nuotare, però non può mai competere con un pesce, perché il pesce nell'acqua è nato e quindi si muove

molto più agevolmente, è il suo ambiente. Questo paragone lo applico anche al digitale, infatti si dice che i nostri figli sono nativi digitali e da loro possiamo imparare grandi lezioni. Quindi io chiedo, perché ho sentito parlare di esempi di questo tipo, se ci sono occasioni nel mondo accademico e universitario di coinvolgimento — oltre che degli studenti che sono iscritti ai corsi — anche delle giovanissime generazioni nel mondo della ricerca e dello sviluppo di innovazioni informatiche.

**RICCARDO TORLONE**, *professore ordinario presso l'Università «Roma tre»*. Ovviamente è un tipo di attività nella quale noi siamo particolarmente interessati. Oltre alla formazione degli studenti, noi tipicamente siamo aperti ai giovani da tanti punti di vista, organizziamo per esempio seminari ed eventi divulgativi aperti al pubblico. Io personalmente organizzo e coordino un evento annuale che si chiama *Data Driven Innovation*, cioè l'innovazione portata dai dati, che è aperto a tutta la popolazione, dove si trattano i temi relativi a questa tematica da tanti punti di vista. Poi voglio citare un'altra iniziativa che è pre-

sente nella mia università, ma sono sicuro che avviene anche nelle altre università. Abbiamo al nostro interno degli incubatori di impresa pensati proprio per favorire la formazione di giovani imprenditori nel settore digitale. Anche questo tipo di attività è assolutamente aperta a tutti, anche se è prevalentemente rivolta agli studenti, e possono contribuire giovani, magari anche senza esperienza tecnica, che però hanno delle idee innovative: messi insieme in un *team* in cui sono presenti anche delle componenti tecniche, riescono a sviluppare delle app che magari possono semplificare proprio la digitalizzazione della pubblica amministrazione e la fruibilità dei dati. Quindi, certamente sì.

**PRESIDENTE**. Grazie. Ringrazio i nostri ospiti, i colleghi e auguro a voi tutti una buona giornata.

Dichiaro conclusa l'audizione.

**La seduta termina alle 9.20.**

---

*Licenziato per la stampa  
il 10 gennaio 2022*

---

STABILIMENTI TIPOGRAFICI CARLO COLOMBO



\*18STC0165000\*