

TESTI ALLEGATI ALL'ORDINE DEL GIORNO
della seduta n. 490 di Martedì 20 aprile 2021

**MOZIONI IN MATERIA DI INFRASTRUTTURE DIGITALI EFFICIENTI E SICURE
PER LA CONSERVAZIONE E L'UTILIZZO DEI DATI DELLA PUBBLICA
AMMINISTRAZIONE**

La Camera,

premessi che:

l'Italia – allineata con il resto dei Paesi europei – ha avviato già da tempo un processo di trasformazione e innovazione dei servizi della pubblica amministrazione attraverso l'utilizzo di tecnologie digitali, spesso però fornite da operatori terzi i quali, mettendo a disposizione le loro infrastrutture, diventano indirettamente detentori di dati e informazioni di esclusivo appannaggio delle amministrazioni interessate;

la costruzione di un *e-government* «autosufficiente», che veda quale obiettivo principale l'accelerazione dei processi di informatizzazione della pubblica amministrazione, in linea con i principi previsti dall'Agenda digitale sia europea che italiana, dalle Comunicazioni della Commissione europea del 26 settembre 2003 e del 19 aprile 2016, nonché dal Piano triennale per l'informatica nella pubblica amministrazione 2020-2022, anche mediante la definizione di un sistema pubblico autonomo nello sviluppo e nell'impiego di tecnologie emergenti, rappresenta un passo fondamentale nella creazione di un più efficiente apparato amministrativo, volto a meglio coniugare l'acquisizione di nuove competenze digitali, con la messa a punto di processi di rafforzamento ed efficientamento dell'azione amministrativa;

in tale contesto, uno degli aspetti più complessi della trasformazione digitale della pubblica amministrazione è dato certamente dalla gestione della vasta e articolata mole di dati che le pubbliche amministrazioni raccolgono e detengono, troppo spesso non ancora in formato digitale;

questa può essere definita come un vero e proprio «patrimonio informativo pubblico», composto da diverse tipologie di informazioni che necessitano di essere collocate all'interno di una strategia complessiva mirata alla loro condivisione, valorizzazione e diffusione tra le amministrazioni pubbliche, siano esse centrali o periferiche;

per realizzare i suddetti obiettivi è necessario che si ceda il passo nella pubblica amministrazione al progresso delle *Information and communication technologies* (Ict), mediante un approccio istituzionale connotato da modalità di gestione più flessibili ed efficaci rispetto al passato;

il ricorso alle Ict nel settore pubblico può infatti agevolare e rendere più efficiente l'attività della pubblica amministrazione e l'interscambio di dati tra le sue articolazioni. Difatti, la diffusa mancanza di interoperabilità tra le varie banche dati della pubblica amministrazione, da intendersi come la capacità delle singole componenti del sistema pubblica amministrazione di fare rete tra loro e dialogare in forma automatica, scambiando informazioni e condividendo risorse, provoca un rallentamento notevole nella messa in atto dell'azione amministrativa, nonché un aggravio inutile dei costi che gravano sul bilancio pubblico, arrivando cioè a determinare inefficacia e inefficienza della stessa;

allo scopo di evitare il protrarsi di questa situazione, è necessaria la creazione di un sistema di infrastrutture di *in cloud computing* per la raccolta e gestione centralizzata dei dati delle pubbliche amministrazioni, che consenta, mediante l'implementazione delle più moderne tecnologie nel settore pubblico – nel rispetto dei principi della trasparenza, efficienza e tutela dei dati personali, così come richiamati dalla normativa europea e nazionale –, di raccogliere, archiviare, elaborare e trasmettere i dati in possesso delle amministrazioni attraverso un cambio di paradigma basato sullo sviluppo di innovative procedure che le tecnologie digitali consentono;

il *cloud computing*, infatti, rappresenta il prerequisito per l'erogazione e la fruizione efficiente di processi e attività come l'archiviazione, l'elaborazione e la trasmissione di dati, mediante la presenza di servizi diversificati e integrati tra loro, quali i cosiddetti IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) e SaaS (*Service as a Service*), ove la disponibilità dei dati è fornita *on demand* attraverso la rete telematica *internet*, a partire da un insieme di risorse preesistenti e configurabili;

sul mercato, esistono numerosi operatori che già permettono ad amministrazioni e aziende, a costi contenuti, di accedere a simili infrastrutture It, prescindendo dal possesso delle strutture a cui vengono materialmente trasferiti i dati. Ciononostante, non può tralasciarsi la necessità, per la pubblica amministrazione, sia di acquisire maggiori competenze in termini di capacità di gestione diretta di siffatte infrastrutture, che di relazione con i principali *player* attivi nell'offerta di tale categoria tecnologica. Tali circostanze, inoltre, si sommano a dubbi legati alla sicurezza, alla *compliance*, alla localizzazione e alla proprietà dei dati, oltre a non lasciare indenne l'amministrazione che si volesse avvalere di tali servizi da eventuali ulteriori rischi quali il «*vendor lock-in*» – ossia la creazione di un rapporto di dipendenza col fornitore del servizio – o il pericolo che fornitori e/o operatori terzi acquisiscano e usino impropriamente dati pubblici. Infine, a fronte dei citati rischi, perdura l'assenza di una reale garanzia in termini di incremento dell'affidabilità dei sistemi, qualità dei servizi erogati e risparmio di spesa;

pertanto, solo mediante la creazione di un sistema infrastrutturale *cloud* di proprietà totalmente pubblica, la cui gestione venga affidata ad un ente pubblico dedicato e/o ad un'azienda pubblica dotata di personale altamente qualificato, sarà possibile far sì che le amministrazioni pubbliche non siano costrette ad avvalersi di fornitori privati per la fruizione di servizi di *cloud storing*. Ciò, inoltre, permetterà di innescare sinergie virtuose capaci di coniugare, al contempo, una maggiore efficienza dell'azione pubblica con elevati *standard* di sicurezza e protezione, così come richiesti dal regolamento generale per la protezione dei dati personali n. 2016/679;

il «Piano triennale per l'informatica nella pubblica amministrazione 2019-2021» ha previsto il censimento del patrimonio Ict delle pubbliche amministrazioni e la procedura di qualificazione dei poli strategici nazionali (Psn). Secondo la circolare n. 1 del 14 giugno 2019 dell'Agenzia per l'Italia digitale per polo strategico nazionale si intende un soggetto titolare dell'insieme di infrastrutture It (centralizzate o distribuite), ad alta disponibilità, di proprietà pubblica, eletto a polo strategico nazionale dalla Presidenza del Consiglio dei ministri e qualificato da Agid ad entrare ad altre amministrazioni, in maniera continuativa e sistematica, servizi infrastrutturali *on-demand*, servizi di *disaster recovery* e *business continuity*, servizi di gestione della sicurezza It ed assistenza ai fruitori dei servizi erogati. Sulla base dei risultati ottenuti a seguito del censimento dei *data center* italiani, è emerso che su 1.252 *data center* censiti, appartenenti a pubbliche amministrazioni centrali e locali, ad aziende sanitarie locali e a università sono solo 35 le strutture candidabili a polo strategico nazionale, 27 sono i *data center* classificati nel gruppo A ovvero con carenze strutturali o organizzative considerate minori e i restanti 1.190 sono stati classificati nel gruppo B, ossia come infrastrutture che non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo o non garantiscono la

continuità dei servizi o non rispettano i requisiti per essere classificati nelle due precedenti categorie;

il decreto-legge 16 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, ha previsto disposizioni dirette a promuovere la realizzazione di un *cloud* nazionale. In particolare, l'articolo 35 stabilisce che, al fine di tutelare l'autonomia tecnologica del Paese, consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni, garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali, la Presidenza del Consiglio dei ministri promuove lo sviluppo di un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale per la razionalizzazione e il consolidamento dei centri per l'elaborazione delle informazioni (ced) destinata a tutte le pubbliche amministrazioni;

con riferimento al rafforzamento della digitalizzazione della pubblica amministrazione, il *Recovery Plan* propone l'obiettivo di razionalizzare e consolidare le infrastrutture digitali esistenti della pubblica amministrazione, promuovendo la diffusione del *cloud computing* e rafforzando la cybersicurezza, con particolare attenzione all'armonizzazione e all'interoperabilità delle piattaforme e dei servizi di dati. Nello specifico al fine di dotare la pubblica amministrazione di infrastrutture affidabili e di accompagnare le amministrazioni centrali verso una nuova logica di conservazione e utilizzo dei dati e di fornitura di servizi, si prevede l'attuazione di un sistema *cloud* efficiente e sicuro. L'obiettivo dell'investimento è, dunque, lo sviluppo sul territorio nazionale di un'infrastruttura affidabile, sicura, efficiente sotto il profilo energetico ed economicamente sostenibile per ospitare i sistemi e i dati della pubblica amministrazione,

impegna il Governo

compatibilmente con i vincoli di finanza pubblica, ad adoperarsi affinché venga creato un sistema di raccolta, conservazione e scambio dei dati della pubblica amministrazione, in precedenza classificati meticolosamente in base alla rilevanza e al livello di sicurezza, mediante lo sviluppo di infrastrutture e sistemi di *cloud computing* di unica proprietà dello Stato, valutando di affidarne la gestione ad un ente pubblico e/o ad un'azienda pubblica, che ne garantisca la sicurezza, la consistenza, l'affidabilità e l'efficienza. (1-00424) (*Nuova formulazione*) «Giarrizzo, Elisa Tripodi, Alaimo, Luciano Cantone, Casa, Scerra, Sodano, Sut, Scanu, D'Orso, Saitta, Rizzo, Penna, Berti, Aresta, Brescia, Maurizio Cattoi, Masi, Alemanno».

(24 febbraio 2021)

La Camera,

premessi che:

la sovranità digitale è uno dei temi chiave per affrontare le sfide della contemporaneità ed assicurare tutela e protezione ai dati dei cittadini;

ovunque si è affermata una compiuta consapevolezza sul ruolo e sul valore dei dati personali prodotti dalle pubbliche amministrazioni e fondati sui dati dei cittadini;

l'Europa, in considerazione dell'assenza di grandi operatori di *cloud* continentali, ha adottato politiche di sviluppo e di rafforzamento del *cloud* europeo;

in Stati come Francia e Germania le politiche del *cloud* relativamente ai dati dei cittadini sono non a caso nelle mani dei rispettivi Ministri dell'economia e delle finanze, Bruno La Maire e Peter Altmaier, a conferma della considerazione che nei due Paesi riscuote il settore dei dati personali dei cittadini come patrimonio della nazione;

le legislazioni di alcuni Paesi prevedono l'obbligo per le loro società nazionali operanti in giro per il mondo di garantire l'accesso alle amministrazioni nazionali per ragioni di sicurezza o di interesse nazionale, come nel caso del «*Cloud Act*» approvato dal Congresso americano nel febbraio 2018;

in considerazione di tali legislazioni invasive, alcuni Paesi hanno immediatamente aggiornato le proprie normative sul *cloud*, come nel caso della Francia, che nel maggio del 2018 ha appositamente modificato la propria legge nazionale sul *cloud*;

l'Italia ha un enorme ritardo rispetto agli altri Paesi europei e ad altri Paesi avanzati esterni all'Unione europea, disponendo in modo limitato di infrastrutture *cloud* nazionali dedicate alla raccolta, custodia e trattamento dei dati;

appaiono a tutt'oggi deboli le politiche pubbliche nazionali di supporto alla creazione di *asset* nazionali di *cloud* sin qui adottate dai precedenti Governi;

le azioni promosse dall'Agenzia per l'Italia digitale in ambito di sviluppo del *cloud* non hanno risposto alle originarie aspettative, dal momento che hanno tradito gli stessi obiettivi previsti dal primo piano triennale 2017-2019 della stessa Agenzia per l'Italia digitale e, in particolare, non sono riuscite a rendere operativi i poli strategici nazionali ideati per soddisfare la domanda pubblica di *cloud* da parte di strutture centrali e periferiche della pubblica amministrazione, purtroppo invece oggi obbligate, in conseguenza di tale grave manchevolezza, a rivolgersi necessariamente ai grandi *player* privati multinazionali che operano sul mercato;

lo sviluppo di società italiane nel settore del *cloud* non è solo un fattore di sovranità e tutela dei dati, ma stimola e sostiene la crescita e la diffusione di competenze digitali nel Paese;

i dati dei cittadini italiani, raccolti e custoditi da pubbliche amministrazioni centrali e locali, a differenza dei dati dei consumatori, devono poter essere affidati a strutture pubbliche e, in caso di insufficienza di queste, a strutture private di nazionalità italiana e con *database* su territorio italiano;

la Costituzione stabilisce, all'articolo 117, che «la potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali (...)» e, alla lettera *r*) del secondo comma, specifica che lo Stato ha legislazione esclusiva sul «(...) coordinamento informativo e informatico dei dati dell'amministrazione statale, regionale e locale (...)»;

l'articolo 117, secondo comma, lettera *r*), indica il contesto per la realizzazione di un *cloud* nelle mani dello Stato che tuteli e protegga i dati prodotti dai cittadini, ma che li usi in modo intelligente come supporto alle decisioni assunte nell'interesse pubblico, con l'obiettivo di migliorare la qualità dei servizi e di istituirne di nuovi;

per adottare tutte le misure, le procedure e le metodologie di uso dei dati come supporto intelligente all'assunzione di decisioni sui servizi destinati ai cittadini, che possono pertanto essere di maggior qualità e di minor costo, occorrono organismi centrali competenti e lungimiranti, attenti

alle evoluzioni delle tecnologie e rispettosi delle prerogative di tutela e protezione dei dati personali;

con l'avvio dei nuovi servizi di 5G e in seguito di 6G, al *cloud* si affiancherà sempre più l'*edge computing*, che sarà necessario sviluppare in modo decentrato e dislocato territorialmente in linea con l'architettura di rete del 5G e 6G;

devono essere adottate con tempestività tutte le misure normative necessarie per assicurare una inversione di tendenza;

nell'ultima Relazione annuale presentata al Parlamento, il Dipartimento delle informazioni per la sicurezza ha rilevato come l'anno della pandemia da COVID-19 sia stato caratterizzato da una minaccia cibernetica sempre più crescente e sofisticata;

in merito, il Rapporto *Clusit* sulla sicurezza Ict in Italia e nel mondo ha rilevato come il 2020 abbia registrato il *record* negativo degli attacchi informatici: a livello globale: sono stati infatti 1.871 gli attacchi gravi di dominio pubblico rilevati nel corso del 2020, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica;

i dati evidenziano, quindi, un'intensificazione degli attacchi sia in termini qualitativi che quantitativi, complice il contesto della pandemia che ha spinto organizzazioni e professionisti a un rapido ricorso alla digitalizzazione,

impegna il Governo:

1) ad adottare iniziative per istituire un organismo di vigilanza, controllo e gestione delle politiche pubbliche sul *cloud* e sulla custodia, tutela e protezione dei dati personali raccolti dalle pubbliche amministrazioni centrali e locali;

2) ad adottare iniziative volte a porre tale organismo in condizione di operare e cooperare in sintonia con il Garante per la protezione dei dati personali e con le università italiane che svolgono attività di ricerca in ambito di raccolta e trattamento dei dati in ambito tecnologico e giuridico;

3) a qualificare, nel più breve tempo possibile, la lista dei poli strategici nazionali, da affiancare a Sogei, impartendo precise direttive all'Agenzia per l'Italia digitale, al fine di recuperare le manchevolezze dell'Agenzia sin qui registrate;

4) ad adottare iniziative, per quanto di competenza, volte a valorizzare le strutture pubbliche di *cloud* oggi gestite dalle locali società *in-house* pubbliche di molte regioni italiane, perché hanno grandi competenze e perché rappresentano l'interlocuzione naturale per le strutture di pubblica amministrazione che cercano fornitori di *cloud* nella stessa regione;

5) ad adottare iniziative di competenza volte a far sì che le aziende private italiane fornitrici di *cloud* e oggi qualificate come *cloud service provider* dalle direttive dell'Agenzia per l'Italia digitale operino nelle loro regioni come riferimenti privilegiati di offerta *cloud* per le strutture di pubblica amministrazione territoriale, affiancando i poli strategici nazionali;

6) nell'ottica di evitare la concentrazione dell'intero patrimonio informativo pubblico in un'unica infrastruttura, con i conseguenti rischi in termini di sicurezza dei dati e dell'infrastruttura stessa, ad assicurare che i dati oggetto di migrazione verso l'infrastruttura unica siano esclusivamente quelli che vengono classificati come critici e strategici, predisponendo a tal fine un'adeguata politica di

catalogazione delle informazioni, che consenta di effettuare valutazioni di impatto, di introdurre un'adeguata etichettatura dei dati in possesso delle pubbliche amministrazioni, di operare decisioni sulla dislocazione dei dati sul territorio nazionale e di predisporre un monitoraggio continuo dei dati delle pubbliche amministrazioni;

7) ad adottare iniziative, anche di carattere normativo, volte a tutelare la sovranità digitale e la sicurezza cibernetica, anche attraverso l'istituzione di un'apposita Agenzia, e a migliorare la qualità dell'architettura di sicurezza della nazione, nonché a costituire un'Agenzia per la competitività, al fine di garantire la sicurezza nazionale e incentivare la promozione di tecnologia nazionale, che possa sostenere l'industria nazionale nei processi di produzione di tecnologia avanzata, evitando la dipendenza tecnologica da nazioni ostili;

8) ad adottare tutte le iniziative di competenza nelle sedi europee affinché sia dato seguito agli intendimenti di cui alla dichiarazione congiunta «*Building the next generation cloud for businesses and the public sector in the EU*», firmata il 15 ottobre 2020 dal Governo italiano e dai Governi di altri 26 Stati europei, assicurando che il progetto per la creazione di un *cloud* federato europeo (Gaia-X) non sia vanificato attraverso il coinvolgimento di soggetti extra-europei, quali *Huawei* e *Alibaba*.

(1-00466) (Nuova formulazione) «Lollobrigida, Meloni, Butti, Mollicone, Albano, Bellucci, Bignami, Bucalo, Caiata, Caretta, Ciaburro, Cirielli, Deidda, Delmastro Delle Vedove, De Toma, Donzelli, Ferro, Foti, Frassinetti, Galantino, Gemmato, Lucaselli, Mantovani, Maschio, Montaruli, Osnato, Prisco, Rampelli, Rizzetto, Rotelli, Rachele Silvestri, Silvestroni, Trancassini, Varchi, Vinci, Zucconi».

(19 aprile 2021)