GRUPPO CONSILIARE LISTA CIVICA ANSELMO SINDACO

Ferrara, 2 dicembre 2025

Al Sig. Sindaco

e p.c. Al Presidente Consiglio Comunale

Oggetto: interpellanza sull'utilizzo di servizi cloud esterni da parte del Comune di Ferrara, rischi per la sovranità digitale e la continuità dei servizi, mappatura delle infrastrutture attualmente in uso.

I sottoscritti consiglieri comunali,

PREMESSO CHE

– il Comune di Ferrara, come tutte le pubbliche amministrazioni, gestisce quotidianamente una mole ingente di dati personali e sensibili (anagrafe, tributi, servizi sociali, servizi educativi, SUAP, attività della Polizia Locale, ecc.), oltre a documenti amministrativi strategici, che devono essere trattati nel rispetto della normativa sulla protezione dei dati personali e con adeguate garanzie di sicurezza, integrità e disponibilità;
– negli ultimi anni molti servizi informatici, inclusi strumenti di produttività individuale (suite d'ufficio, posta elettronica, condivisione documenti, videoconferenza), vengono sempre più spesso erogati in modalità cloud da fornitori esterni, prevalentemente privati e per lo più extra-UE;
– risulta che almeno il servizio di posta elettronica dell'Ente sia attualmente affidato a un fornitore esterno in modalità cloud (con conseguente memorizzazione dei contenuti delle comunicazioni e dei metadati su infrastrutture non direttamente gestite dal Comune);

CONSIDERATO CHE

– autorevoli analisi giornalistiche e tecniche hanno recentemente richiamato l'attenzione sul fatto che circa il 70% dell'infrastruttura cloud europea è oggi in mano a tre grandi fornitori statunitensi (Google, Microsoft, Amazon), mentre solo una quota minoritaria è gestita da operatori europei, con evidenti implicazioni in termini di dipendenza tecnologica e di sovranità digitale;
– tale dipendenza espone le istituzioni europee, e quindi anche le amministrazioni locali che utilizzano tali servizi, a rischi non solo tecnici (guasti, attacchi informatici), ma anche geopolitici e giuridici, poiché le società fornitrici sono soggette a norme del loro Stato di appartenenza (come lo US Cloud Act) che consentono alle autorità statunitensi un ampio

potere di accesso e di intervento sui dati custoditi nei loro server, inclusi quelli relativi a clienti pubblici europei;
– in scenari non più puramente teorici, è stato ipotizzato e discusso a livello europeo il rischio che una futura amministrazione statunitense possa usare il controllo delle grandi piattaforme cloud come leva politica, arrivando – in casi estremi – a imporre limitazioni o interruzioni del servizio verso governi e istituzioni dei Paesi ritenuti "non allineati", con effetti potenzialmente devastanti sulla continuità di funzioni essenziali (servizi sanitari, finanziari, amministrativi, giudiziari);
– lo stesso dibattito pubblico si è arricchito di casi concreti nei quali istituzioni europee o internazionali hanno subito improvvise interruzioni nell'accesso ai propri servizi di posta e ai propri conti, in un contesto di tensioni politiche e sanzioni, a testimonianza della delicatezza del legame fra infrastrutture digitali critiche e contesto geopolitico;
- in particolare è stato riportato dalla stampa come il Procuratore Capo della Corte Penale Internazionale abbia trovato sospeso il proprio account mail istituzionale, a seguito di un ordine esecutivo del Presidente degli Stati Uniti che imponeva sanzioni contro i funzionari della stessa ICC e che successivamente la stessa Corte abbia deciso di spostare i propri Servizi applicative su una piattaforma open source europea;

TENUTO CONTO CHE

– i principali fornitori di software di produttività stanno modificando il funzionamento delle applicazioni da ufficio largamente utilizzate anche nelle amministrazioni pubbliche, impostando come predefinito il salvataggio automatico dei documenti nel cloud anziché in locale sui dispositivi dell'utente;
– ciò comporta che, anche in assenza di scelte consapevoli da parte degli utilizzatori, documenti di lavoro, bozze, allegati e file che possono contenere dati particolarmente delicati (dati sanitari, sociali, giudiziari, economici, ecc.) finiscano sistematicamente su infrastrutture remote, sulle quali l'Ente potrebbe non avere un controllo pieno e diretto, e che potrebbero essere soggette a trattamento automatizzato, anche tramite strumenti di intelligenza artificiale, secondo condizioni contrattuali spesso poco chiare e mutevoli nel tempo;
– gli esperti di sicurezza informatica richiamano inoltre il rischio di fenomeni di lock-in tecnologico (dipendenza da un singolo fornitore o da un ristretto oligopolio) che rendono difficile, costoso e talvolta quasi impraticabile migrare verso soluzioni alternative più sicure o più rispettose della sovranità dei dati dell'Ente;

CONSIDERATO INOLTRE CHE

– alcuni Stati europei e diverse istituzioni stanno già sperimentando percorsi di progressiva riduzione della dipendenza da fornitori extra-UE, puntando sulla costruzione di un "cloud sovrano" e sull'adozione di software libero e open source;
– in Olanda il Parlamento ha formalmente chiesto al governo di ridurre drasticamente la dipendenza dai servizi informatici statunitensi, qualificandoli come una minaccia potenziale all'autonomia e alla sicurezza informatica nazionale, e analoghe sollecitazioni sono emerse in Germania, Danimarca e in altri Paesi europei;
– l'Italia, come Stato membro dell'Unione Europea, è chiamata a tenere in considerazione tali orientamenti nell'organizzazione dei propri servizi pubblici e nella scelta delle infrastrutture digitali da utilizzare, anche a livello locale;

RITENUTO CHE

– per un Comune come Ferrara è ormai questione strategica dotarsi di una chiara mappatura dei servizi digitali critici e delle infrastrutture tecnologiche utilizzate, verificando dove siano fisicamente localizzati i dati, quali soggetti abbiano potenzialmente accesso agli stessi, quali siano le garanzie contrattuali in materia di protezione dei dati, continuità del servizio, tutela rispetto a richieste di accesso da parte di autorità straniere;
– sia necessario valutare, in un'ottica di medio-lungo periodo, scenari che prevedano una progressiva riduzione della dipendenza da fornitori cloud esterni extra-UE almeno per i servizi più critici, privilegiando ove possibile soluzioni basate su infrastrutture interne, consortili o comunque sotto controllo europeo, nonché su software libero e standard aperti;

TUTTO CIÒ PREMESSO

interpellano il Sindaco e la Giunta per sapere:
1. Quali servizi informatici del Comune di Ferrara siano attualmente erogati in modalità cloud da fornitori esterni, specificando per ciascuno:
- denominazione del servizio (es. posta elettronica, gestione documentale, condivisione file, videoconferenza, piattaforme per procedimenti amministrativi, servizi scolastici, tributi ecc.);
- fornitore;
- sede legale del fornitore e area geografica prevalente di localizzazione dei dati (UE, SEE, extra-UE);
- principali basi giuridiche e contrattuali che regolano il trattamento dei dati e le garanzie in materia di protezione, riservatezza, disponibilità.

2. Se, oltre alla posta elettronica, esistano altri servizi core dell'Ente (in particolare gestione documentale, protocollo, anagrafe, servizi sociali, sistemi di pagamento e di rendicontazione, sistemi di gestione del personale, piattaforme di comunicazione interna) che si appoggiano a infrastrutture cloud esterne non gestite direttamente o indirettamente dalla Pubblica Amministrazione italiana o europea e, in caso affermativo, di quali servizi si tratti.

3. Se siano state effettuate, e con quali esiti, valutazioni d'impatto sulla protezione dei dati (DPIA) ai sensi del GDPR, in relazione all'utilizzo di servizi cloud forniti da soggetti extra-UE o comunque sottoposti a normative come lo US Cloud Act, nonché se siano previste specifiche clausole contrattuali per tutelare l'Ente rispetto a richieste di accesso ai dati da parte di autorità straniere.

4. Quali misure siano attualmente in vigore per garantire la continuità operativa dei servizi essenziali dell'Ente in caso di improvvisa indisponibilità, anche prolungata, dei servizi cloud esterni (ad esempio per decisione unilaterale del fornitore, per attacchi informatici, per eventi geopolitici o per sanzioni):
- esistenza di piani di business continuity e disaster recovery aggiornati;
- frequenza e modalità di backup locali (su infrastrutture interne o comunque sotto controllo dell'Ente);
- possibilità tecnica di migrare in tempi rapidi verso fornitori alternativi o verso infrastrutture interne.

5. Se il Comune abbia avviato o intenda avviare un percorso di analisi comparativa sull'adozione di soluzioni alternative, in particolare:
- servizi cloud erogati da soggetti pubblici o consortili italiani/europei;

- piattaforme basate su software libero e open source per la produttività individuale e la collaborazione (suite d'ufficio, posta, calendario, condivisione file, videoconferenza), analoghe a quelle già adottate in alcuni Länder tedeschi o ministeri europei;
- a che punto sia l'implementazione nei Servizi utilizzati dall'amministrazione del progetto di cloud regionale guidato da Lepida che dovrebbe consentire di condividere infrastrutture tra enti pubblici mantenendo la sovranità sui dati.

6. Se sia stata svolta una valutazione del rischio specifico relativo all'uso di funzionalità di intelligenza artificiale integrate nei servizi cloud utilizzati dal Comune, in particolare rispetto:
- all'eventuale utilizzo dei dati dell'Ente per l'addestramento di modelli di IA dei fornitori;
- al rischio che contenuti sensibili possano essere "rigurgitati" da tali sistemi in contesti non appropriati;
- alle clausole contrattuali che disciplinano questi aspetti e alle eventuali limitazioni o disattivazioni di tali funzionalità da parte dell'Ente.

7. Se l'Amministrazione ritenga opportuno definire e rendere pubblico un "piano comunale per la sovranità digitale", che individui obiettivi, tempi e tappe per:
- mappare e classificare tutti i servizi digitali critici e i fornitori utilizzati;
- ridurre gradualmente la dipendenza da infrastrutture cloud extra-UE per i dati più sensibili;
- aumentare l'uso di software libero e standard aperti;
- rafforzare le competenze interne del personale sull'uso consapevole di strumenti cloud e sulla gestione dei dati.

Si chiede, infine, che le informazioni richieste vengano rese disponibili anche in forma di documento pubblico, fruibile sul sito istituzionale del Comune, al fine di garantire massima trasparenza ai cittadini e alle cittadine sulle scelte in materia di infrastrutture digitali e servizi cloud.

I consiglieri comunali Gruppo Consiliare Lista Civica Anselmo Sindaco:

Leonardo Fiorentini

Fabio Anselmo

Arianna Poli