Viviamo in un'epoca di profonda trasformazione storica. La competizione geopolitica globale non si limita più ai confini fisici, alle rotte commerciali o alle riserve energetiche. Si estende al mondo dei dati, delle infrastrutture digitali e alla capacità di controllare i flussi di informazione e i modelli di intelligenza artificiale che influenzano sempre più le decisioni critiche per la vita dei cittadini e della società.

Quando si parla di tutele, negli ultimi vent'anni l'Europa ha sviluppato un'ampia regolamentazione: dal GDPR, per la protezione dei dati personali, all'AI Act in tema di intelligenza artificiale, fino alla NIS2 in materia di cyber sicurezza, ma non ha ancora raggiunto l'autonomia tecnologica necessaria a garantirne l'efficacia.

La dipendenza tecnologica dell'Europa è una realtà tangibile e misurabile. I dati sanitari dei cittadini europei, per esempio, transitano su cloud soggetti a normative extra UE. I modelli di intelligenza artificiale che supportano le decisioni pubbliche vengono addestrati su infrastrutture non direttamente gestite dalla pubblica amministrazione (PA). Le amministrazioni pubbliche, inoltre, stipulano contratti con fornitori che nel tempo rischiano di diventare insostituibili, non per la loro superiorità, ma per la mancanza di alternative generando lock-in tecnologico. Questa dipendenza strutturale riduce la capacità di decidere autonomamente nell'interesse dei propri cittadini.

Il presente *Decalogo per la Sovranità Digitale* nasce in questo contesto, non come esercizio teorico o manifesto ideologico, ma come strumento pratico e operativo per chi, nelle pubbliche amministrazioni, nelle istituzioni, nelle imprese e nella società civile ha la responsabilità e la volontà di invertire questa tendenza. Non si chiede l'isolamento dal mercato globale né il rifiuto delle tecnologie più avanzate, ma l'applicazione di principi: che ogni scelta tecnologica sia valutata in base all'interesse collettivo, che ogni sistema sia progettato per rimanere sotto controllo e che ogni dipendenza sia governata e ridotta nel tempo con metodo e determinazione.

I *dieci principi* delineati in questo documento non costituiscono semplici slogan, ma indicazioni operative di rilevanza strategica. Essi trattano la progettazione di architetture modulari per l'implementazione dell'intelligenza artificiale mantenendo il controllo sui dati, l'aggregazione delle

risorse per progetti open source, la formazione di personale pubblico affinché sia dotato delle competenze necessarie per una governance efficace dei sistemi e, non ultimo, la federazione di infrastrutture cloud tra diverse amministrazioni, per ottimizzare le risorse senza incrementare le dipendenze. In questo quadro, viene posta particolare attenzione alla sostenibilità economica ed ecologica delle scelte tecnologiche, attraverso la promozione di soluzioni che riducano costi e impatti ambientali nel lungo periodo.

Ogni principio contenuto nel Decalogo trae origine dall'esperienza pratica di professionisti che hanno già affrontato tali problematiche e hanno sviluppato soluzioni replicabili.

Adottare questo Decalogo implica riconoscere che la sovranità digitale non è un argomento tecnico riservato agli esperti IT, ma un elemento che riguarda la società nel suo insieme. Significa affermare che i dati generati da cittadini e istituzioni pubbliche sono un bene comune, che appartengono a tutti gli individui che fanno parte dell'Unione Europea. Significa optare per l'investimento in competenze interne, codici e modelli aperti, e infrastrutture resilienti. Non perché sia la soluzione più facile nel breve termine, ma perché è l'unica in grado di assicurare autonomia e sostenibilità a lungo termine.

Per questo, il Decalogo si rivolge principalmente alle *pubbliche amministrazioni* di ogni livello. Sono loro i primi custodi del *patrimonio digitale collettivo*, i primi responsabili della protezione dei dati della cittadinanza e i primi a subire le conseguenze di scelte tecnologiche non ponderate. Il Decalogo si rivolge anche alle *Università* e ai *centri di ricerca* che formano le competenze del futuro, alle *imprese private* che collaborano con (e per) il settore pubblico, alle associazioni di categoria e alla società civile. Tutti soggetti che hanno il diritto e il dovere di partecipare a questa trasformazione.

La sovranità digitale europea non si raggiunge con un'unica legge o un'unica infrastruttura, ma attraverso migliaia di scelte quotidiane, coerenti e guidate da principi condivisi a tutti i livelli e in tutte le fasi: dalla progettazione allo sviluppo e al rilascio delle applicazioni finali. Il principio della condivisione deve guidare tutto il processo.

Questo Decalogo vuole essere un passo concreto verso la piena attuazione di scelte condivise: è un impegno verso tutti gli individui, le istituzioni e le generazioni future che si troveranno a usare l'infrastruttura digitale che stiamo costruendo oggi.

L'Europa ha già proposto le regole di riferimento, adesso è arrivato il momento di prepararci alle sfide geopolitiche future e guidare nella giusta direzione la progettazione di una nuova generazione di sistemi pubblici.

Il Decalogo della Sovranità Digitale

10 punti inderogabili e pratici per un ecosistema autonomo, sicuro, responsabile e proiettato verso un futuro sostenibile ed equilibrato.

1. *GOVERNA L'IMPIANTO APPLICATIVO E TECNOLOGICO*[1]

Controlla direttamente ogni aspetto dei tuoi servizi: *data center*, *infrastrutture*, *piattaforme abilitanti*, *strumenti di osservabilità*, *applicazioni* e *dati*. Questo controllo si estende a tutte le componenti, anche quelle di terze parti, e richiede una gestione dell'intera catena del valore. Rivaluta periodicamente la dipendenza da fornitori critici, verificando il mantenimento del controllo e della disponibilità dei dati per evitare dipendenze non evidenti.

Mantieni un inventario aggiornato di componenti critiche, dei fornitori e delle dipendenze, identificando chiaramente chi ne detiene il controllo operativo, tecnico e contrattuale. Verifica, inoltre, l'esistenza di funzioni non documentate o dipendenze non sostituibili, definendo per ogni componente essenziale un piano di uscita, migrazione o sostituzione.

2. *PUNTA SU STANDARD APERTI*

Privilegia l'adozione di standard aperti nello sviluppo di applicazioni e nell'interazione con piattaforme e infrastrutture di mercato. Questo approccio consente alle pubbliche amministrazioni di non legarsi a un singolo *vendor*[2] evitando casi di *lock-in*[3] o cambiamenti commerciali che rendano oneroso l'utilizzo di una specifica soluzione.

Il software libero è lo strumento di trasparenza per eccellenza, in quanto consente la verifica indipendente della sicurezza, l'accesso a un'ampia platea di fornitori e la crescita delle competenze interne, anche attraverso la collaborazione con imprese e atenei del territorio.

Quando possibile, quindi, privilegia l'utilizzo di piattaforme open source[4] e/o soluzioni che permettano evoluzione, supporto e subentro. In termini operativi questo richiede di adottare interfacce applicative (API[5]) documentate e formati aperti di dati, evitare componenti proprietari non esportabili, valutare portabilità e costi di uscita già nelle fasi di procurement e garantire accesso a documentazione tecnica.

---

[1] Impianto applicativo e tecnologico (stack tecnologico): combinazione strutturata di tecnologie, software e strumenti interdipendenti utilizzati per sviluppare, eseguire e gestire un'applicazione o un sistema informatico.

[2] Vendor: fornitore di tecnologie, piattaforme o soluzioni digitali; azienda che offre prodotti e/o servizi (spesso software o hardware) a organizzazioni clienti, talvolta includendo supporto, manutenzione e consulenza.

[3] Lock-in (vendor lock-in): dipendenza vincolante da un fornitore che rende tecnicamente o economicamente proibitivo il passaggio ad altre soluzioni.

[4] Open source: software il cui codice sorgente è accessibile, permettendo verifica indipendente, modifica e indipendenza dai singoli fornitori.

[5] API (Application Programming Interface): insieme di regole e protocolli che permette a programmi diversi di comunicare e scambiarsi dati e funzionalità in modo standardizzato.

3. *RIDUCI L'ESPOSIZIONE DEI DATI A NORMATIVE E ACCESSI DI PAESI TERZI*

Crea soluzioni tecniche e adotta presidi giuridici per proteggere le informazioni e la conoscenza generate, conservate e gestite digitalmente dalle istituzioni e degli organismi europei, prevenendo la loro esposizione a tecnologie o regole non conformi alla normativa UE.

Per esempio, adotta sistemi di cifratura *end-to-end* con chiavi generate da sistemi europei o, meglio ancora, *on-premise*[6]. Prevedi clausole contrattuali che garantiscano l'applicazione della normativa nazionale e dell'Unione Europea. Struttura forme di collaborazione interne agli enti e tra gli enti per rafforzare la forza contrattuale rispetto a vendor globali e ridurre la necessità di ricorrere a soluzioni non governate. L'obiettivo è assicurare che i dati, la conoscenza, le informazioni e le competenze rimangano nel perimetro tecnico e giuridico dell'Unione.

4. *AUMENTA L'INDIPENDENZA TECNOLOGICA*

Ricorda che ogni sistema pubblico dovrebbe essere costruito come un insieme di componenti separabili, con interfacce chiare e responsabilità distinte, in modo da evitare dipendenze tecniche non reversibili. Operativamente, questo significa separare dati, logica applicativa, orchestrazione, gestione delle identità e interfacce utente; evitare personalizzazioni che leghino in modo irreversibile un componente al resto del sistema e prevedere verifiche periodiche di sostituzione o migrazione di componenti critici. Questo eviterà che il cambio di un fornitore comporti la ricostruzione completa della piattaforma o della soluzione.

5. *PROMUOVI UNA IA RESPONSABILE*

Progetta una Intelligenza Artificiale (IA) nella pubblica amministrazione separando nettamente dati, basi di conoscenza, modelli, decisioni e orchestrazione. Non è solo una scelta tecnica: è una condizione abilitante per la sovranità digitale e la conformità normativa.

Mantieni sotto controllo diretto basi documentali, indici, log applicativi e metadati di utilizzo. Classifica *prompt*[7] e dati in ingresso prima di inviarli a qualsiasi modello esterno, e ricorri a modelli esterni solo per casi compatibili con il livello di sensibilità del dato, applicando regole di minimizzazione, anonimizzazione e codifica.

Privilegia modelli IA specializzati, ove possibile, più "leggeri" ed erogabili anche su infrastrutture locali, per ridurre la dipendenza esclusiva dalla capacità elaborativa degli *hyperscaler*[8].

[6] On-premise: modello in cui software, dati e infrastruttura IT sono installati e gestiti localmente nei server dell'organizzazione, che ne mantiene controllo diretto, sicurezza e manutenzione, in alternativa al cloud.

[7] Prompt: input (domanda o istruzione in linguaggio naturale) che l'utente fornisce a un sistema di intelligenza artificiale per guidare la generazione della risposta o dell'output.

[8] Un hyperscaler è un'azienda che gestisce infrastrutture cloud e di calcolo a scala enormemente grande: decine o centinaia di migliaia di server distribuiti in datacenter in tutto il mondo.

6. *INVESTI IN FORMAZIONE*

Prevedi percorsi di formazione del personale sulle competenze critiche: cybersecurity, architettura dei sistemi e gestione di infrastrutture e dati. Queste funzioni non possono essere delegate interamente a fornitori esterni, per evitare la perdita del controllo diretto su ciò che si governa. È importante prevedere il trasferimento di conoscenza obbligatorio nei progetti affidati a terzi. Chi commissiona un sistema senza capirlo non è in grado di valutarlo, verificarlo o sostituirlo. Le competenze interne devono crescere insieme alla complessità dei sistemi gestiti, perché ogni nuova piattaforma adottata richiede un corrispondente investimento in formazione.

7. *GARANTISCI DISPONIBILITÀ, RESILIENZA E CONTINUITÀ OPERATIVA*

Garantisci il controllo completo di infrastrutture e servizi, in modo che siano fungibili anche in maniera modulare, distribuendo i sistemi critici su infrastrutture ridondanti e geograficamente separate. Crisi geopolitiche, cambi di strategia del mercato, attacchi informatici o disastri naturali non sono scenari remoti, ma rischi concreti da anticipare.

Imposta i progetti tenendo conto che ci devono essere forme di ridondanza non solo tecniche e organizzative, ma anche contrattuali: la resilienza non si improvvisa durante la crisi, si costruisce prima, pezzo per pezzo.

8. *GOVERNA L'USO DEI DATI DELLA PUBBLICA AMMINISTRAZIONE*

Individua i tuoi asset digitali di valore (dati personali, database in generale, ecc.) e struttura strumenti tecnico-giuridici di difesa. Esigi sempre il pieno rispetto del GDPR e della normativa a tutela delle banche dati e prevedi strumenti contrattuali capaci di prevenire il verificarsi di situazioni critiche.

Preserva la conoscenza da utilizzi non controllati guidandone l'uso per il pubblico interesse, sia che si tratti di addestramento di modelli IA, sia di profilazione, ricerca o semplice redistribuzione.

9. *PUNTA ALLA MASSIMA CONDIVISIONE*

Fai in modo di condividere, replicare e migliorare collettivamente ogni soluzione sviluppata con successo da un'amministrazione. Crea piattaforme e soluzioni funzionali a valorizzare e sostenere l'altruismo dei dati e la condivisione di modelli, soluzioni e competenze seguendo tre obiettivi fondamentali.

Il primo è diffondere attivamente le esperienze di successo tra enti pubblici, evitando che ogni amministrazione riparta da zero. Il secondo è favorire la nascita di ecosistemi di servizi pubblici interoperabili e collaborativi, in cui componenti sviluppate da soggetti diversi operino su standard comuni. E, infine, come terzo obiettivo, favorisci la costruzione di infrastrutture cloud federate, per consentire la condivisione sicura di risorse e servizi tra amministrazioni mantenendo piena sovranità sui dati.

La collaborazione tra pubbliche amministrazioni non è un valore astratto: è il moltiplicatore che trasforma esperienze locali in patrimonio collettivo.

10. *ORIENTA OGNI DECISIONE TECNOLOGICA A VANTAGGIO DEL BENE COMUNE*

Tieni conto che ogni scelta tecnologica pubblica va valutata prima di tutto in base all'impatto diretto sui cittadini, garantendo trasparenza delle scelte tecnologiche.

Questo vale per qualsiasi decisione: quale piattaforma adottare, dove conservare i dati, quale fornitore selezionare. In pratica, significa introdurre criteri espliciti di valutazione dell'interesse pubblico nei processi di progettazione e di acquisto, analizzare il lock-in, i costi di uscita e la portabilità, ma anche verificare che nessuna soluzione concentri eccessivo potere tecnico, economico o informativo in un singolo soggetto.

Se la tecnologia è uno strumento, il bene comune costituisce la bussola che deve orientare ogni decisione a riguardo.

Il decalogo, in linea con i principi dell'Agenda 2030 per lo Sviluppo Sostenibile, si fonda sulla su una visione green e sostenibile.