

Intelligenza artificiale e PA: questioni aperte

Barbara Marchetti, Nicoletta Rangone*

ARTIFICIAL INTELLIGENCE AND THE PUBLIC SECTOR: OUTSTANDING ISSUES

ABSTRACT: This paper builds on a report on artificial intelligence and public administration produced as part of an Astrid research project and examines a number of specific issues concerning, in particular, internal governance, administrative planning, transparency and access to algorithms, the assessment of environmental costs, and the exchange of best practices among public administrations. It concludes by highlighting both the strengths and the shortcomings of the current phase of experimentation with and deployment of artificial intelligence by public authorities.

KEYWORDS: public administration; artificial intelligence; governance; transparency; procurement

ABSTRACT: Il contributo muove da un rapporto su IA e pubblica amministrazione condotto nell'ambito di una ricerca Astrid ed esamina taluni profili specifici riguardanti, in particolare, la governance interna, la programmazione, il tema della trasparenza e dell'accesso all'algoritmo, la valutazione dei costi ambientali e lo scambio di buone pratiche tra amministrazioni. In conclusione, si mettono in luce luci ed ombre dell'attuale fase di sperimentazione e impiego dell'IA da parte delle pubbliche autorità.

PAROLE CHIAVE: pubblica amministrazione; intelligenza artificiale; governance; trasparenza; *procurement*

SOMMARIO: 1. Introduzione – 2. Fattori da considerare per progettare le sperimentazioni e gli usi – 3. La scelta tra *in-house* e mercato: verso una maggiore autonomia tecnologica? – 4. Quale governance interna per l'IA? – 5. Gli interessi da tutelare nel caso di ricorso al mercato – 6. Quale coordinamento tra amministrazioni? – 7. Un bilancio di luci ed ombre.

* Barbara Marchetti: professoressa di diritto amministrativo nell'Università di Trento, Mail: barbara.marchetti@unitn.it. Nicoletta Rangone: professoressa di diritto amministrativo nell'Università Lumsa. Mail: n.rangone@lumsa.it. Seppure frutto di una riflessione comune, i paragrafi 3, 4 e 5 sono stati redatti da Barbara Marchetti e i paragrafi 1 e 2 da Nicoletta Rangone. Il presente contributo è stato realizzato nell'ambito delle attività del Centro di Eccellenza Jean Monnet "Sustainable Artificial Intelligence for Regulation" (SUSTAIN-AI-REG), progetto n. 101240897, co-finanziato dall'Unione Europea nell'ambito del Programma Erasmus+ (Azioni Jean Monnet). Contributo sottoposto a referaggio anonimo.

1. Introduzione

I dati raccolti con i questionari e in occasione dei *focus group* consentono di intravedere aspetti non del tutto esplorati e risolti nei rapporti tra autorità pubbliche e uso dell'IA, per i quali mancano (ancora) prassi comuni e percorsi paralleli di riflessione. Proviamo ad indicare qui i profili che ci sembrano di sicura rilevanza.

2. Fattori da considerare per progettare le sperimentazioni e gli usi

Nel valutare se avviare una sperimentazione o mettere a regime l'uso di un sistema di IA andrebbe circostanziata, in primo luogo, «l'esigenza da soddisfare, gli obiettivi da raggiungere e l'effettiva necessità di soddisfare tale esigenza attraverso sistemi di IA»¹.

In caso di valutazione di effettiva necessità del ricorso all'IA, andrebbe sciolto il nodo della *proporzionalità*² della scelta rispetto alle esigenze e agli obiettivi da raggiungere. A quest'ultimo riguardo, ad esempio, da un lato modelli più piccoli in termini di dimensioni e complessità potrebbero essere più facilmente producibili *in house* o acquisibili in riuso, presentando il vantaggio di un minor consumo computazionale, dunque risultare interessanti anche da un punto di vista del ridotto impatto ambientale, e della "sovranità", poiché nessun dato verrebbe condiviso con servizi ospitati all'estero; dall'altro, sistemi prodotti *in house* potrebbero risultare meno performanti rispetto a certi prodotti commerciali che hanno anche accesso a risorse di calcolo quasi illimitate³.

E qui veniamo al secondo punto. Nel valutare se avviare una sperimentazione o mettere a regime l'uso di un sistema di IA andrebbe considerata *l'esistenza o meno di sperimentazioni/usi simili e della loro funzionalità rispetto agli obiettivi a seguito di monitoraggio*, che si tratti del *drafting* di documenti (su cui ha lavorato, ad esempio, il Senato)⁴ o della valutazione del rischio nei controlli (su cui rileva l'esperienza di Regione Lombardia già nel 2022)⁵.

¹ «You should select the most appropriate technology to meet your needs. (...) However, you should also be open to the conclusion that, sometimes, AI is not the best solution for your problem: it may be more easily solved with more established technologies» (Government Digital Services, , *Artificial Intelligence Playbook for the UK Government*, Guidance, 2025, <https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government/artificial-intelligence-playbook-for-the-uk-government.html#principle-8-you-work-with-commercial-colleagues-from-the-start>).

² Il rispetto del criterio di proporzionalità è richiamato nelle linee guida Agid nel principio 2.3.1 *Tutela dei diritti fondamentali, trasparenza, proporzionalità e non discriminazione* in cui si prevede che i sistemi di IA siano progettati e utilizzati nel pieno rispetto dei diritti fondamentali, evitando effetti discriminatori e garantendo un livello di trasparenza e proporzionalità adeguato al contesto d'uso. Il medesimo principio, tuttavia, viene poi declinato nel senso che «Le misure adottate per rispettare i principi del presente paragrafo devono essere proporzionate al contesto di utilizzo e agli obiettivi del sistema, anche tenuto conto degli esiti delle valutazioni preventive (di impatto sui diritti fondamentali e in tema di protezione dei dati personali).

³ «To assess the trade-off between sovereignty, security and quality, relevant practical experience must first be gathered» (P. BIEGELBAUER, A. SCHINDLER, R. CONDE JIMÉNEZ, P. WEINLINGER, *Exciting Opportunities and Necessary Safeguards for Large Language Models in the Public Sector*, in *ERCIM News*, 136, 2024, 25-26. <https://doi.org/https://ercim-news.ercim.eu/en136>).

⁴ Ufficio valutazione impatto, *L'intelligenza artificiale in Senato Sperimentazioni, opportunità e risultati nelle diverse fasi del processo legislativo*, documento di analisi n. 34, 2025.

⁵ La Regione Lombardia «ha ideato un algoritmo per la classificazione, ex post e in base al rischio, delle imprese alimentari. Tale classificazione è utilizzata per valutare e revisionare la programmazione dei controlli in materia di



Ciò consentirebbe, peraltro, di sapere «come altri soggetti pubblici hanno affrontato i vincoli che interessano tutte le pubbliche amministrazioni», come la spiegabilità delle decisioni su cui interviene l'IA o la protezione dei dati pubblici. A puro titolo esemplificativo, gli strumenti di IA predisposti e utilizzati da Banca d'Italia per la gestione degli esposti dei clienti nelle relazioni con le banche e gli intermediari finanziari⁶ e la relativa disciplina sul trattamento dei dati personali⁷ potrebbero ispirare le attività di altre amministrazioni con funzioni di vigilanza, come l'Autorità per le garanzie nelle comunicazioni-AGCOM, che ha attivato una piattaforma per la risoluzione delle controversie tra utenti e operatori di telefonia e di servizi di media audiovisivi (ConciliaWeb)⁸, o l'Autorità di regolazione dei trasporti-ART con riferimento al Sistema Telematico di acquisizione reclami dei passeggeri che viaggiano nell'ambito dell'Unione europea su treni, autobus, navi e aerei, che lamentano la violazione dei diritti riconosciuti dalla normativa europea⁹.

La mappatura di sperimentazioni/usi simili permetterebbe tra l'altro di «verificare se esistono sistemi riutilizzabili» in quanto concepiti in *open source*¹⁰. Il riuso, previsto in via obbligatoria a livello nazionale¹¹ ed

sicurezza alimentare su tutta la Regione. Di particolare rilevanza, la capacità dell'algoritmo di adattarsi alle possibili variabili e modulare il livello di rischio a sostituzione della categorizzazione standard utilizzata sino a quel momento. Il calcolo del livello di rischio delle imprese tramite l'algoritmo rappresenta uno strumento gestionale per organizzare efficacemente le risorse disponibili e rendere più efficace l'attività di controllo. Inoltre, la pratica si distingue per la trasparenza nella rappresentazione dei dati usati e del relativo aggiornamento, per l'economicità del processo e la flessibilità dello strumento in virtù della sua adattabilità alle esigenze e al territorio" (L. MEGALE, *Buone Pratiche Regolatorie: le esperienze italiane*, in *Rassegna trimestrale dell'Osservatorio AIR*, XIII/4, 2022, 29). Tale pratica è stata premiata nell'ambito del già nell'ambito del "Contest buone pratiche regolatorie" realizzato nel 2022 dalla Cattedra Jean Monnet on European Approach to Better Regulation della LUMSA, in collaborazione con l'Osservatorio AIR e con il patrocinio del Ministro per la pubblica amministrazione e dell'OCSE.

⁶ Per una descrizione delle modalità di funzionamento dell'algoritmo, nonché delle misure tecniche e organizzative adottate per un uso dell'innovazione etico, responsabile e conforme alle norme, si veda M. ELIA, *Regolamentare l'Intelligenza Artificiale, tra l'uso di machine learning e la protezione dei dati personali: l'esperienza della Banca d'Italia*, in *Rassegna trimestrale dell'Osservatorio AIR*, XIII-4, 2022, 33 ss.

⁷ Regolamento concernente il trattamento dei dati personali effettuato dalla Banca d'Italia nell'ambito della gestione degli esposti riguardanti la trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari e clienti e i diritti e gli obblighi delle parti nella prestazione dei servizi di pagamento, 22 marzo 2022. Per un commento, si veda M.B. ARMIENTO, *Prove di regolazione dell'intelligenza artificiale: il regolamento della banca d'Italia sulla gestione degli esposti*, in *Giornale di diritto amministrativo*, 1, 2023, 103 ss.

⁸ <https://conciliaweb.agcom.it/conciliaweb/login.htm>.

⁹ <https://www.autorita-trasporti.it/site/>.

¹⁰ JoinUp è una piattaforma volta a facilitare lo scambio e il riuso di soluzioni IT per le pubbliche amministrazioni, finanziato dalla Commissione europea nel 2016 attraverso il programma "Interoperability Solutions for public administrations, businesses and citizens" -ISA2 (<https://interoperable-europe.ec.europa.eu/interoperable-europe>). Questa piattaforma ospita il Public Sector Tech Watch, un Osservatorio della Commissione europea volto al monitoraggio e alla disseminazione degli usi di tecnologie emergenti nelle PA, come l'IA e la blockchain (<https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch>).

¹¹ "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali" (art. 69, comma 1, d.lgs. 7 marzo 2005, n. 82, Codice delle amministrazioni digitali).

europeo¹², è disciplinato da apposite linee guida AGID¹³, dal piano triennale per l'informatica nella PA¹⁴ ed è previsto da vari piani regionali per la riorganizzazione digitale, ad esempio quello della Puglia. Come già evidenziato, il riuso presenta anche una serie di ricadute positive in termini di risparmi economici («consentendo di colmare il gap strutturale interno») ed energetici (ed in generale ambientali, *infra*); infine il riuso, riducendo potenzialmente il ricorso al mercato, limiterebbe anche i rischi connessi in termini di protezione dei dati pubblici, preservando la sovranità digitale¹⁵ (*infra* par. 2).

In secondo luogo, già in fase di sperimentazione sarebbe importante avere contezza della *categoria in cui potenzialmente rientra il sistema di IA*: se si tratta di un sistema ad alto rischio (con le regolazioni stringenti che ne derivano) o a rischio minimo (con limitati obblighi di trasparenza), oppure se il sistema – benché ricompreso tra quelli elencati dall'art. 5 del regolamento Ue 2024/1689 e dunque vietato – presenti le caratteristiche che ne consentono lo sviluppo e l'impiego (perché, ad esempio, è «un sistema di IA per la valutazione o la classificazione delle persone fisiche» -social scoring- il cui punteggio venga applicato esclusivamente nei «contesti in cui i dati sono stati originariamente generati»)¹⁶. Si tratta di attività che le PA devono necessariamente compiere, in base alle previsioni europee, in caso di sviluppo *in house* di un sistema; diversamente la classificazione compete al provider (*infra* par. 3). Una classificazione operata in fase di sperimentazione controllata consentirebbe, peraltro, di progettare un sistema di IA già coerente con le garanzie previste a livello europeo (ad esempio in termini di garanzia del controllo umano, nonché di pertinenza e rappresentatività dei dati)¹⁷.

Quando l'amministrazione sperimenta/sviluppa *in house* il sistema, è poi fondamentale «distinguere tra attività sostanziali e ancillari/preparatorie rispetto all'attività amministrativa avente rilevanza esterna»¹⁸, dato che il regolamento europeo prevede al riguardo un'eccezione all'applicazione delle regole previste per i sistemi ad alto rischio¹⁹, ma rispetto alle quali va comunque assicurata la trasparenza (*infra* par. 5). Si tratta di una classificazione alquanto complessa e sensibile in quanto, in taluni casi, lo svolgimento di attività ancillari potrebbe comunque influenzare in modo sostanziale l'attività finale: si pensi al caso di un sistema di IA che svolga un compito preparatorio nella determinazione del paese di origine il quale, in

¹² Communication to the European Commission, *Open Source Software Strategy 2020 – 2023*, C(2020) 7149 final. A gennaio 2026, la Commissione ha pubblicato una *call for evidence* sulla «strategia europea per un ecosistema digitale», volta a definire «un approccio strategico al settore open source nell'UE che affronti l'importanza dell'open source quale contributo fondamentale alla sovranità tecnologica, alla sicurezza e alla competitività dell'UE; un quadro strategico e operativo per rafforzare l'uso, lo sviluppo e il riutilizzo delle risorse digitali aperte all'interno della Commissione, sulla base dei risultati conseguiti nell'ambito della strategia della Commissione in materia di software open source per il periodo 2020-2023» (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-Ecosistemi-digitali-aperti-europei_it).

¹³ AGID, *Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni*, 2019.

¹⁴ AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione*, Edizione 2024-2026. Aggiornamento 2026.

¹⁵ AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione*, 68-69 e 76.

¹⁶ Art. 5, comma 1, lett. c, i.

¹⁷ A questo riguardo, le linee guida AGID per lo sviluppo dell'intelligenza artificiale nella pubblica amministrazione, attualmente in consultazione, sono chiare nell'affermare che «In fase di sviluppo, i sistemi di IA DEVONO essere progettati secondo il principio di compliance by design, includendo requisiti normativi (AI Act, GDPR, New Legislative Framework - NLF) lungo l'intero ciclo di vita» (principio 1).

¹⁸ Vale a dire «compiti procedurali ristretti», tesi «a migliorare il risultato di un'attività umana», a rilevare deviazioni da precedenti decisioni umane ma non volti a sostituirla senza revisione umana, o ancora compiti preparatori.

¹⁹ Art. 6, comma 3, regolamento Ue 2024/1689.



caso di malfunzionamento, potrebbe comportare un rischio per il godimento (la tutela) del diritto di asilo²⁰.

In terzo luogo, andrebbe preso in considerazione «l'impatto ambientale della sperimentazione. Andrebbe, ad esempio considerata la necessità di una sperimentazione» (in termini generali, oppure *ex novo* rispetto ad una che adatta – in riuso - un sistema esistente) e la sua *proporzionalità*, considerando anche i costi ambientali²¹. Detto questo, non si può ignorare l'assenza (al momento in cui si scrive) di un sistema condiviso di misurazione dell'impatto ambientale e delle componenti da prendere in considerazione²², né il regolamento europeo impone vincoli stringenti in tal senso²³. Ciononostante, sembra possibile rivolgere alle amministrazioni alcune indicazioni generali, limitatamente all'uso efficiente dell'energia²⁴. Occorrerebbe, in particolare, distinguere tra consumi dei data center per *training* o *tuning* dei sistemi di IA e quelli legati al funzionamento dei sistemi di IA (*AI inference*). Con riferimento ai primi, non vi è dubbio che costi energetici variano per le amministrazioni che si sono dotate di data center (come INPS e Corte dei conti), che “vedono” più chiaramente i consumi energetici (anche se poi questi difficilmente possono essere ripartiti per le singole applicazioni), rispetto a quelle che ne sono prive e sperimentano in *cloud* (per le quali i costi energetici sono sostenuti in ampia misura dal *cloud provider*). In entrambe le ipotesi, per limitare

²⁰ European Union Agency for Fundamental Rights, *Assessing high-risk artificial intelligence: fundamental right risks. Report*, Vienna, 2025, 8. I rischi connessi ad un abuso dell'auto-classificazione da parte delle PA degli usi di IA come preparatori, che comporta la non applicazione delle garanzie previste per i sistemi ad alto rischio, è evidenziato dall'European Data Protection Supervisor, *Preparing the EU PA for the AI Act*, 2025, 15.

²¹ «Public and private Institutions (...) should create a 'proportionality framework' to assess whether training or tuning of an AI model for a particular task is proportional to the carbon footprint, and general environmental impact, of that training and/or tuning. This is especially true with AI projects used by the state» (A. VAN WYNSBERGHE, *Sustainable AI: AI for sustainability and the sustainability of AI*, in *AI and Ethics*, 1, 2021, 217).

²² Per quantificare il consumo di energia dell'IA generativa, alcuni metodi si basano sulla presunzione dell'energia usata dai server alla luce dei consumi di quelli più diffusi (così A. DE VRIES, *The growing energy footprint of artificial intelligence*, in *Joule*, 7, 2023), altri misurano la domanda di energia per una determinata richiesta (come la produzione di un testo o di un'immagine) attraverso un apposito software Python (Code Carbon) che consente al computer dell'utente di accedere alle specifiche tecniche dei chip che eseguono il modello nel centro dati e fornisce una stima di quanta energia è stata consumata (S. CHEN, *AI's energy problem*, in *Nature*, 639, 6 marzo 2025, 23). Vale osservare che si tratta comunque di stime approssimative, che non tengono conto del training e del fatto che è difficile isolare l'energia usata dai data center per la sola IA generativa ed assumono l'utilizzo di un determinato server (NVIDIA).

²³ Ad oggi mancano disposizioni vincolanti a tutela dell'ambiente e le misure non vincolanti rischiano di non essere sufficienti a sostenere in modo efficace la sostenibilità ambientale. In particolare, la standardizzazione tende a concentrarsi soprattutto sui consumi energetici, trascurando altri tipi di consumi e ulteriori impatti; analogamente, i codici di condotta, pur orientati a definire indicatori chiave per valutare e ridurre l'impatto ambientale dei sistemi di IA, risentono della loro natura non cogente e potrebbero focalizzarsi anch'essi solo sui consumi energetici. Mancano, infine, obblighi di trasparenza estesi a tutti i consumi (non solo energetici) e non risultano adeguatamente considerate applicazioni diverse da quelle ad alto rischio e dai modelli a finalità generale (N. RANGONE, *Intelligenza artificiale, tutela dell'ambiente e regolazione europea*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2025, 547-548; L. PARONA, *La ponderazione dei costi ambientali nell'approvvigionamento di sistemi di intelligenza artificiale da parte delle amministrazioni pubbliche*, in *BioLaw Journal – Rivista di Biodiritto*, 1, 2025, 549-569; B. MARCHETTI, *I costi ambientali nascosti dell'intelligenza artificiale*, in *Blog Diario di diritto pubblico*, 5 maggio 2024, <https://www.diariodidirittopubblico.it/i-costi-ambientali-nascosti-dellintelligenza-artificiale/>.

²⁴ Di sostenibilità energetica parlano le già citate linee guida Agid: «In fase di sviluppo, i sistemi DEVONO essere progettati tenendo conto dell'efficienza energetica e computazionale, privilegiando modelli proporzionati» (principio 18); si veda anche par. 3.1.1.1 Energy Layer e par. da 4.1 a 4.5. Di valutazione dei costi ambientali parlano anche le linee guida AgID in materia di procurement di IA.

gli impatti ambientali, è auspicabile che i data center gestiti *in house* o a cui si fa indirettamente ricorso attraverso servizi in *cloud* siano alimentati con fonti rinnovabili ed utilizzino tecnologie di alimentazione e raffreddamento all'avanguardia (che assicurano «economie di scala, massimizzando l'ottimizzazione e l'utilizzo di hardware e processi efficienti»)²⁵. «L'uso dell'*edge computing* consente inoltre di ridurre la dipendenza dai data center centralizzati, migliorando l'efficienza ambientale complessiva»²⁶.

Quanto all'impatto ambientale dei connessi al funzionamento dei sistemi di IA, assumono rilievo le tecnologie di IA. Ad esempio, nello sviluppo di sistemi a disposizione dei giudici amministrativi²⁷, il Segretario generale della giustizia amministrativa ha fatto ricorso «a un processo specifico, di quantizzazione, che determina una riduzione della precisione dei dati senza però comportare rilevanti ricadute sulla significatività degli stessi, con il vantaggio di una contrazione dei consumi energetici»²⁸. Occorre anche distinguere tra *training* e uso a regime, dato che la prima fase è caratterizzata da una significativa intensità di consumi²⁹, senza però dimenticare che consumo energetico cumulativo delle inferenze potrebbe risultare addirittura superiore³⁰. A tale riguardo, ad esempio, la Lombardia effettua un benchmarking dei modelli a più basso impatto ambientale, come quelli che fanno uso di sistemi RAG (generazione potenziata da recupero), che ottimizzano gli LLM attraverso l'accesso a banche dati non utilizzate per il *training*, riducendo così l'esigenza di riallenare il modello con dati nuovi in sede di adattamento ad un uso specifico di una PA (dunque risparmiando risorse computazionali). In generale, una stima ragionevolmente attendibile dei consumi di elettricità associati alle applicazioni di IA operative su infrastrutture server e cloud può essere desunta dal codice alfanumerico che si trova in bolletta (POD), seppure tali informazioni restituiscano di norma un quadro aggregato e richiedono un'adeguata ripartizione per attribuire i consumi al singolo modello IA effettivamente in esecuzione.

²⁵ B. BRUNO, N. BARDINO, D.F. SIVILLI, *Intelligenza artificiale e Giustizia amministrativa: strategie di impiego, metodologie e sicurezza*, 2024, 7, in <https://www.giustizia-amministrativa.it/-/152174-350>.

²⁶ Aspen Institute Italia - Osservatorio Permanente sull'Adozione e l'Integrazione della Intelligenza Artificiale (IA2), *Rapporto Intelligenza Artificiale – 2025*, 2025, 162.

²⁷ Volti, in particolare, all'identificazione di ricorsi correlati o simili pendenti nelle singole Sezioni, alla ricerca dei precedenti giurisprudenziali con uno strumento basato sia parole chiave, che sulla rilevazione di connessioni semantiche; alla rilevazione e possibilità di visualizzazione immediata delle norme o delle pronunce della giurisprudenza indicate in un atto difensivo (B. BRUNO, N. BARDINO, D.F. SIVILLI, *Intelligenza artificiale e Giustizia amministrativa: strategie di impiego, metodologie e sicurezza*, cit., 8).

²⁸ «La quantizzazione consiste nel convertire i pesi e le attivazioni delle reti neurali da numeri in virgola mobile a numeri interi con larghezza di *bit* inferiore. Sebbene possa, in linea teorica, influenzare la precisione dei modelli di *machine learning* (specie nei modelli che usano il *deep learning*), è spesso necessaria per ridurre la quantità di memoria e la potenza di calcolo e, di conseguenza, ridurre l'impatto energetico» (B. BRUNO, N. BARDINO, D.F. SIVILLI, *Intelligenza artificiale e Giustizia amministrativa: strategie di impiego, metodologie e sicurezza*, cit., 19).

²⁹ Si stima che «GPT-4 (2023) e LLaMA 3.1 405B (2024) hanno raggiunto rispettivamente 5.184 e 8.930 tonnellate di CO₂, evidenziando una tendenza crescente nell'impatto ambientale dovuto ai processi di addestramento. (...) [Al contempo] il progetto cinese DeepSeek ha lanciato una sfida alla "corsa ai parametri" dei LLM. La release DeepSeek-V3 (febbraio 2025) impiega un'architettura *Mixture-of-Experts* con 671 miliardi di parametri totali, ma soltanto 37 miliardi attivi per *token*, contenendo l'addestramento in circa 2,8 milioni di ore-GPU H800 e in un *budget* inferiore ai sei milioni di dollari, a parità di *performance* con modelli assai più energivori. Il caso DeepSeek dimostra che ridimensionare i modelli senza sacrificare le prestazioni è possibile e apre la strada a una "IA frugale" con minore impronta carbonica» (Aspen Institute Italia - Osservatorio Permanente sull'Adozione e l'Integrazione della Intelligenza Artificiale (IA2), *Rapporto Intelligenza Artificiale – 2025*, cit., 156).

³⁰ N. ALDER, K. EBERT, R. HERBRICH, P. HACKER, *AI, Climate, and Transparency: Operationalising and Improving the AI Act*, in *Journal of European Consumer and Market Law*, 14(4), 2025, 166 ss.



In quarto luogo, già in fase di sperimentazione (o di bando per l'acquisto in *outsourcing*) andrebbe impostato il *monitoraggio e la valutazione ex post* del funzionamento dei sistemi (come nel caso di INPS)³¹. Questa fase è importante sia per una costante rivalutazione della necessità del ricorso a un sistema di IA, ma anche per rilevare deviazioni rispetto agli obiettivi o possibili ottimizzazioni (anche *infra* par. 3). A questo fine, occorre definire obiettivi e indicatori.

3. La scelta tra *in-house* e mercato: verso una maggiore autonomia tecnologica?

La sperimentazione/produzione *in house* consente all'amministrazione di guidare la progettazione tecnica dei sistemi, soprattutto se si creano team interdisciplinari, ad esempio, tra funzionari che useranno i sistemi e computer scientist, come da tempo in Banca d'Italia e Consob (*infra* par. 3). Questo approccio assicura una funzionalità del prodotto alle esigenze dell'amministrazione stessa, così come il rispetto dei vincoli che si impongono agli usi dell'IA nelle pubbliche amministrazioni³².

Al contempo, la sperimentazione/produzione *in house* consente un controllo sui dati non paragonabile a quanto deriva da un *outsourcing* non adeguatamente disciplinato in sede di bando (*infra* par. 4), oppure dall'uso di soluzioni standard offerte sul mercato (ad esempio Copilot-Microsoft o Gemini-Google).

Varie amministrazioni fanno ricorso a soluzioni di mercato (in modo esclusivo o misto) per diverse ragioni, che vanno dalla mancanza di risorse umane e/o fisiche (come data center), all'offerta da parte di fornitori esterni di *performance* superiori sul piano computazionale rispetto a opzioni interne, alla fidelizzazione che si crea rispetto al provider che fornisce all'amministrazione altri servizi (come quello di posta elettronica), che è in grado per questo di fare offerte molto convenienti su applicazioni di IA e che confida anche sull'effetto di inerzia/*status quo bias* dell'amministrazione.

A ciò si aggiungano le strategie di ingresso massiccio in determinati comparti, come quello universitario, che solo grandi provider sono in grado di realizzare; ne è un esempio la sottoscrizione nel 2025 di un contratto tra OpenAI e la Conferenza dei Rettori delle Università Italiane-CRUI, a seguito di procedura negoziata senza previa pubblicazione di un bando di gara³³, per la fornitura triennale di ChatGPT a tutti i docenti di università italiane, statali e non. È presumibile che, al termine dei tre anni, se la convenzione non verrà rinnovata, varie università stipuleranno a loro volta contratti con OpenAI per assicurare ai docenti la continuità del servizio. Nella stessa direzione di facilitare rapporti di fidelizzazione va la stipula dell'accordo tra Open AI e l'Università Bocconi per l'offerta di «strumenti di intelligenza artificiale specia-

³¹ Per l'organizzazione del monitoraggio, ad esempio attraverso audit interni, e i fattori da monitorare si veda il par. 4.6 delle citate linee guida AGID.

³² L'approccio *regulation by design*, «aims to embed regulatory objectives directly into technological architectures, making design choices a vehicle for achieving social governance of systems. (...) The design of AI systems involves encoding legislation into software (...), meaning that design decisions about input features, data types, and human-AI interactions become policy decisions that are no longer delegated to public deliberation but rather to third-party developers» (T. SCHMUDE, T. LE GOFF, M. YURRITA, K. ALFRINK, S. TSCHIATSCHEK, T. VIARD, *Two Means to an End Goal: Connecting Explainability and Contestability in the Regulation of Public Sector AI*, forthcoming <https://arxiv.org/abs/2504.18236>).

³³ Ex art. 76, comma 2, lett b), d.lgs. n. 36/2023, come emerge dal sito CRUI, nel quale non è indicato l'importo pagato, <https://www.crui.it/bandi-di-gara-e-contratti-pubblici/procedura-negoziata-openai.html>.

lizzati per il mondo accademico all'intera comunità composta da 17.000 studenti, docenti e staff»³⁴. Vi è da chiedersi se prima della stipula siano state considerate altre offerte di fornitori italiani (come Almagest)³⁵ o di altri paesi europei, anche in considerazione della "delicatezza" dei dati raccolti dalle università³⁶. Ad esempio, l'Università di Padova ha messo a disposizione, il primo strumento di IA generativa realizzato da un'università statale (Lucrezia-IA)³⁷, ma pur sempre basato sul modello Claude di Anthropic. Alcuni paesi europei stanno seguendo direzioni opposte. In Francia, il ministro dell'istruzione ha rifiutato le offerte gratuite di Microsoft Office 365 e Google Workspace per le scuole³⁸. A livello europeo, la decisione del Garante per la protezione dei dati-EDPS in base alla quale l'uso da parte della Commissione europea di Microsoft 365 (che annovera anche servizi di IA come Copilot) sarebbe stata in contrasto con la disciplina europea a protezione dati³⁹, ha portato a una profonda revisione dell'accordo con la società e ad una decisione di chiusura del procedimento senza rilievi⁴⁰. La Commissione ha vietato l'uso di ChatGPT e messo a disposizione dei suoi funzionari un apposito tool GPT@EC⁴¹; vi è da dire, però, che questa chatbot si appoggia a GPT-4-Turbo o GPT-4-o di OpenAI, Llama 3.1 8b di Meta e Nous Hermes 2 Mixtral 8x7B DPO⁴², dunque sistemi non sviluppati da società europee. Seppure le amministrazioni tendano ad essere consapevoli del trade-off tra sovranità tecnologica e capacità operativa, è auspicabile anche a questo riguardo una conoscenza reciproca delle soluzioni adottate e

³⁴ <https://www.unibocconi.it/it/argomento-news/openai>. Con ogni probabilità, l'acquisizione è stata effettuata senza gara, trattandosi di una università non statale, che il Consiglio di Stato ha considerato non rientranti tra le amministrazioni aggiudicatrici (comm. spec., 26 ottobre 2018, n. 2427).

³⁵ I modelli di IA Velvet sono stati progettati e realizzati integralmente in Italia, addestrati sull'infrastruttura di supercalcolo Leonardo di Cineca. «La famiglia comprende sia modelli enterprise hosted sia modelli open weights: le versioni enterprise estendono le migliori capacità a contesti regolamentati, mentre i modelli open-weights riflettono il forte impegno di Almagest verso lo sviluppo open-source» (<https://www.almagest.com/it/tecnologia/velvet/>)

³⁶ OpenAI dichiara (nell'interfaccia di ChatGPT) che «non utilizza i dati dell'area di lavoro [università] EDU per addestrare i modelli», e questo è una buona cosa, ma i dati (anche personali) si trovano comunque su cloud e sono processati da data center collocati fuori dall'Europa e dunque non regolati dalla disciplina europea. Alcune università hanno già predisposto indicazioni al riguardo che evidenziano chiaramente che «inserire dati personali nei prompt può portare a violazioni del GDPR, con potenziali conseguenze legali per l'ateneo» (così le Linee guida per l'utilizzo dell'intelligenza artificiale nella didattica, nella ricerca e nei processi amministrativi; nella stessa direzione quelle dell'Università di Verona).

³⁷ <https://lucrezia.unipd.it/>.

³⁸ <https://www.agendadigitale.eu/sicurezza/privacy/mantovani-m5s-no-a-microsoft-e-google-nelle-scuole-seguiamo-lesempio-della-francia/>.

³⁹ European Data Protection Supervisor, investigation into use of Microsoft 365 by the European Commission (Case 2021-0518), decision (8 March 2024).

⁴⁰ European Data Protection Supervisor rileva che, a seguito della modifica del «Data Protection Terms of the Inter-Institutional Licensing Agreement with Microsoft regarding the Commission's use of Microsoft 365», i dati vengono trattati solo per fornire i servizi alla Commissione europea e ogni ulteriore trattamento è ammesso solo in casi compatibili e conformi al diritto europeo, i trasferimenti di dati personali verso Paesi terzi sono circoscritti, non vi saranno divulgazione arbitrarie dei dati personali da parte di autorità o terzi (WRW/SS/ak/ D(2025) 2636 - C 2021-0518, Closure of enforcement proceedings in the Commission's use of Microsoft 365, Case 2021-0518).

⁴¹ In linea con gli obiettivi delineati dalla Comunicazione della Commissione europea, *Artificial Intelligence in the European Commission (AI@EC) A strategic vision to foster the development and use of lawful, safe and trustworthy Artificial Intelligence systems in the European Commission*, C(2024) 380 final.

⁴² «L'ente ha fatto sapere di non aver intrattenuto corrispondenza con gli sviluppatori dei modelli di AI in vista di una loro adozione, né di aver siglato contratti specifici o accordi per la riservatezza delle informazioni» (<https://www.wired.it/article/intelligenza-artificiale-chatbot-commissione-europea/>).





dei problemi affrontati. Al contempo, come evidenziato da Agid, «la portabilità dei sistemi di IA e la possibilità di esecuzione su hardware eterogeneo assumono una valenza strategica» sono centrali al fine di «ridurre il rischio di lock-in tecnologico; aumentare la resilienza rispetto a vincoli di mercato o di approvvigionamento; favorire la nascita e il consolidamento di una filiera locale e nazionale dell'IA»⁴³. Inoltre, il ricorso a soluzioni di mercato potrebbe essere superato da una regia che finanzia lo sviluppo di soluzioni condivise, a livello regionale o nazionale e – in prospettiva – europeo (cfr. anche par. 5). In tema di “AI sovereignty”⁴⁴, sarebbe infine cruciale una cooperazione tra pubbliche amministrazioni per lo sviluppo di data center e cloud pubblici, utili a un insieme di PA, operanti – ad esempio, a livello regionale o centrale –, così come la realizzazione di data center o cloud europei⁴⁵ o localizzati in Europa e chiare indicazioni per la preferenza di questi rispetto a soluzioni extraeuropee.

4. Quale governance interna per l'IA?

L'indagine rileva l'istituzione presso alcune amministrazioni di uffici/unità competenti ad adottare le decisioni in materia di programmazione e progettazione di sistemi di IA. Si tratta tuttavia di ipotesi ancora marginali, poiché in molti casi la valutazione circa l'opportunità di procurarsi sistemi di IA, di svilupparli in house o di acquistarli sul mercato, di impiegarli per determinate funzioni e non per altre è lasciato principalmente al personale tecnico informatico⁴⁶.

Ciò che avviene è cioè una separazione tra l'individuazione della necessità di un'applicazione, che è operata dai funzionari di missione o dalla dirigenza amministrativa, e la ricerca concreta di tale applicazione, demandata alla componente tecnica, che ricerca il modello efficiente per lo svolgimento di quel compito. In realtà, come accennato *supra* (par. 2), le valutazioni in ordine alla acquisizione e all'utilizzo di applicazioni di IA sono di natura complessa e richiederebbero un confronto interdisciplinare tra diversi saperi e competenze: accanto alla expertise tecnico-informatica e di *data analysis*, sarebbe, infatti, auspicabile la presenza di personale in grado di valutare l'impatto dei sistemi per quanto concerne il rispetto della disciplina dei dati e il contenimento dei rischi per la sicurezza ed i diritti fondamentali, dato il noto problema dei *bias*. Del resto, il regolamento europeo prevede espressamente la necessità di una valutazione di im-

⁴³ Par. 6.3, Linee guida citate.

⁴⁴ The World Economic Forum, in collaboration with AI Global Alliance, *Rethinking AI Sovereignty: Pathways to Competitiveness through Strategic Investments*, white paper, January 2026.

⁴⁵ Al momento, in linea con la proposta del rapporto Draghi “The future of European competitiveness” (2024, p. 82), è stato proposto un Cloud and AI Development Act (di cui è stata pubblicata l'analisi di impatto); il *Next Generation Internet programme* (<https://ngi.eu/>) offre, invece, sostegno finanziario allo sviluppo di soluzioni digitali decentralizzate open-source. Nel 2025 è inoltre stato costituito un consorzio (*Digital Commons European Digital Infrastructure Consortium*) dedicato ai “beni comuni digitali”, che «riunisce amministrazioni pubbliche, comunità Open Source e aziende per mettere in comune le risorse, sostenere componenti strategiche aperte e accelerare la transizione da progetti pilota isolati a infrastrutture digitali condivise e scalabili» (<https://digital-strategy.ec.europa.eu/it/news/digital-commons-edic-launches-advance-europes-technological-sovereignty>). Interessante anche il progetto di AI gigafactories, vale a dire data center dedicati allo sviluppo di modelli avanzati, la cui costituzione a livello europeo si vorrebbe supportare attraverso una modifica del regolamento n. 2021/117, che disciplina le attività dell'impresa comune per il calcolo ad alte prestazioni europeo-EuroHPC.

⁴⁶ Si può altresì rilevare, incidentalmente, che questa tendenza parrebbe rafforzata dal tenore di molte delle linee guida AgID, le quali presentano un contenuto tecnico difficilmente comprensibile a chi manchi di competenze informatiche specifiche.

patto sui diritti fondamentali (quantomeno per i sistemi ad alto rischio) come obbligo per il *deployer* pubblico (art. 27), il quale deve altresì assicurare che i dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità (specifica) prevista dal sistema di IA ad alto rischio (art. 26)⁴⁷.

Le valutazioni diventano ancora più complesse, e richiedono a maggior ragione un dialogo tra diverse competenze, quando l'amministrazione sviluppa *in house* il sistema, considerato l'obbligo stabilito in capo ai provider di operare la classificazione del rischio e, nelle ipotesi in cui si ravvisino le condizioni di alto rischio, di assicurare altresì la compliance ai numerosi requisiti stabiliti dagli artt. 9-15 e relativi alla gestione dei rischi (art. 9), alla qualità dei dati (art. 10), alla trasparenza sufficiente del sistema (art. 13), alla sorveglianza umana (art. 14) e alla sua adeguata accuratezza e robustezza (art. 15)⁴⁸.

Di qui la sicura opportunità, soprattutto per le amministrazioni complesse e di dimensioni significative (amministrazioni centrali dello Stato, grandi città, regioni, autorità indipendenti) di costituire unità ad hoc in cui convergano funzionari dotati delle diverse competenze.

La valutazione dei rischi in termini di diritti e di privacy dovrebbe sommarsi poi ad un'analisi più complessiva in termini di *costi/benefici*, la quale accanto alle ragioni di efficienza e di economicità (che sappiamo trainare la spinta all'IA) sappia considerare attentamente sia i costi economico/finanziari necessari per dotarsi dell'IA (anche dal punto di vista energetico ed ambientale), sia i rischi che la traslazione di attività valutative umane in procedimenti automatizzate comporta. Ad esempio, come dimostra l'importante rapporto *Extreme Poverty and Human Rights* di Philip Alston alle Nazioni Unite, con riferimento al caso SyRI olandese⁴⁹, errori nei procedimenti per l'assegnazione di contributi e sussidi pubblici (in quello che viene chiamato *Digital Welfare State*) hanno un impatto molto forte in termini di conseguenze negative per le fasce più deboli della popolazione, ciò che dovrebbe orientare le amministrazioni ad una automatizzazione di tali procedimenti solo a fronte di sistemi trasparenti e con un altissimo grado di accuratezza. Mentre un diverso bilanciamento potrebbe caratterizzare l'impiego dell'IA in settori meno delicati e sensibili: si pensi all'impiego di sistemi per estrarre conoscenza dai dati al fine di orientare una policy pubblica

⁴⁷ In questi termini v. p. 29 delle linee guida AgID di prossima pubblicazione, scaricabili all'indirizzo https://www.agid.gov.it/sites/agid/files/2025-02/Linee_Guida_adozione_IA_nella_PA.pdf, adottate nell'ambito del Piano triennale per l'informatica della pubblica amministrazione 2024-2026.

⁴⁸ Per riferimenti anche alle esperienze straniere v. F. DECAROLIS, B. MARCHETTI, L. TORCHIA, *The EU Digital Regulation and its Impact on Member States*, Cham, 2025.

⁴⁹ Nel caso dell'algoritmo olandese SyRI, prima citato, all'incirca 26000 famiglie sono state falsamente accusate di frode tra il 2005 e il 2019 dalle autorità fiscali olandesi in ragione di algoritmi discriminatori. Sono stati creati dei profili di rischio per coloro che richiedevano benefits statali in cui "foreign-sounding names" e "dual nationality" erano usati come indicatori di possibile frode fiscale. Migliaia di famiglie a basso-medio reddito sono state sottoposte a controlli, sono state erroneamente accusate di frode ed è stato chiesto loro di restituire denaro che avevano avuto legittimamente, che in qualche caso ammontava a migliaia di euro. Con la conseguenza che molte famiglie hanno contratto debiti, sono diventate povere e in qualche caso hanno perso lavoro e casa. Più di 1000 bambini, di conseguenza, sono stati affidati ai Servizi sociali (The European Parliament, 2022). Un paper pubblicato nell'ottobre 2025 (U. AJUZIEOGU, *Due process in Automated Government benefit Determination: A Constitutional Framework for Algorithmic Governance in the Administrative State*, https://www.researchgate.net/publication/395703184_Due_Process_in_Automated_Government_Benefit_Determination_A_Constitutional_Framework_for_Algorithmic_Governance_in_the_Administrative_State) denuncia attraverso un'analisi empirica di 800 casi documentati l'estrema fallibilità dei sistemi automatici di attribuzione dei benefits in 23 diverse esperienze statali. Sul caso SyRI v. A. RACHOVITSA, N. JOHANN, *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons learned from the Dutch SyRI Case*, in *Human Rights Law Review*, 2022, 22.



o ai sistemi IA di tipo conversazionale, per la gestione di chatbot, in cui le conseguenze legate ad eventuali inaccuratezze sono maggiormente tollerabili.

A questo proposito, occorrerebbe chiarirsi su un punto decisivo. Quando si motiva il ricorso all'IA con ragioni di efficienza, dovrebbe essere chiaro che questa non deve essere intesa tanto in termini di risparmio di risorse organizzative o di personale per l'amministrazione, ma di capacità del sistema di offrire servizi migliori ai cittadini⁵⁰. Il bilanciamento operato a monte, quindi, deve essere tra benefici per la *collettività* e possibili rischi per la stessa, e non incentrarsi sul risparmio per l'amministrazione in sé considerata.

Ancora, una valutazione rigorosa del sistema in fase di programmazione dovrebbe comprendere una valutazione della accuratezza dell'algoritmo e della sua robustezza tecnica, da commisurare al compito svolto e al grado di controllabilità umana. Sempre in questa logica, e benché i sistemi più performanti siano anche i meno spiegabili, l'amministrazione dovrebbe eventualmente rinunciare all'impiego di sistemi ML se, a causa della c.d. black box, si determinasse una contrazione inammissibile delle garanzie legate alla motivazione e alla sindacabilità delle decisioni pubbliche. Del resto, la mancata considerazione di tale fondamentale aspetto avrebbe come conseguenza un rischio estremamente elevato di annullamento giurisdizionale per l'impossibilità di assicurare quelle garanzie minime che il Consiglio di Stato ha enucleato nella propria giurisprudenza sulla nota vicenda del piano straordinario di mobilità dei docenti⁵¹. Sempre in questa logica, che muove dalla complessità e dalla centralità delle decisioni da prendere in fase di programmazione, andrebbe inserita, come ricordato in precedenza nel par. 2, la valutazione dei costi ambientali. Nonostante le difficoltà ancora esistenti in ordine alla misurazione di tali costi, come rilevato *supra*, si tratta di un elemento non più procrastinabile da inserire nell'analisi costi/benefici complessiva, la cui mancata considerazione potrebbe tradursi presto in termini di costi per la singola amministrazione e di crisi energetica europea, se si considerano i dati sull'incremento di fabbisogno energetico per l'IA secondo le stime dell'Agenzia mondiale dell'energia⁵².

⁵⁰ In questi termini pare particolarmente interessante rifarsi al Rapporto del 2022 che il Consiglio di Stato francese ha redatto, su richiesta dell'allora Primo Ministro Jean Castex, dal titolo *Intelligence artificielle et action publique: construire la confiance, servir la performance* (<https://www.conseil-etat.fr/publications-colloques/etudes/etudes-a-la-demande-du-gouvernement/intelligence-artificielle-et-action-publique-construire-la-confiance-servir-la-performance>).

⁵¹ Si tratta delle note pronunce 2270/2019 e 881/2020 che, come è noto, hanno precisato come l'ingresso di tali strumenti nella funzione pubblica non possa significare sottrazione delle decisioni algoritmiche ad un regime di pubblicità e di *explainability*. Il Consiglio di Stato, non potendo applicare alla decisione prodotta da un algoritmo le garanzie della legge 241/90, ha individuato nuove garanzie, traendole dal Regolamento europeo per la tutela dei dati personali (General Data Protection Regulation, d'ora in avanti GDPR), rappresentate *dalla piena conoscibilità dell'algoritmo*, *dalla imputabilità all'organo titolare del potere dei suoi output*, *dalla garanzia del controllo umano* e *dal divieto di effetti discriminatori*. In argomento, cfr. A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 2019, 4; P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination Under EU Law*, in *CMLR*, 2018, 55, 1143; B. CASEY, A. FARHANGI, R. VOGL, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, in *Berkeley Technology Law J.*, 2019, 34:143, 144; S. WATCHER *et al.*, *Why a Right to explanation of Automated Decision-making Does Not Exist in the General Data Protection Regulation*, in *Int'l Data Privacy L.*, 2017, 76.

⁵² I data center raddoppieranno l'attuale consumo energetico (pari all'1,5 % del consumo mondiale di energia elettrica) entro il 2023. Il report completo della International Energy Agency è scaricabile da <https://iea.blob.core.windows.net/assets/de9dea13-b07d-42c5-a398-d1b3ae17d866/EnergysandAI.pdf>.

Questo stesso team interdisciplinare dovrebbe essere chiamato anche a svolgere il monitoraggio del sistema nell'intero ciclo di vita, così da poterne misurare ex post costi e benefici, rischi discriminatori e ricadute positive per i cittadini. Le linee guida AgID sull'IA sono sul punto chiare, esigendo dalla amministrazione una capacità di governo dei sistemi per l'intero ciclo di vita dell'IA.

5. Gli interessi da tutelare nel caso di ricorso al mercato

Per le ragioni riportate *supra*, la decisione su come procurarsi un sistema di IA appare cruciale.

Già si è detto che la scelta dell'*in-house* andrebbe, quando possibile, preferita per varie ragioni, prima fra tutte la conservazione dei dati in un ambiente protetto e l'autonomia digitale. Tuttavia, essa non appare sempre percorribile, sia in ragione delle più alte performance assicurate dalle società private fornitrici in termini di soluzioni tecnologiche sia per la mancanza di adeguate competenze informatiche nelle amministrazioni pubbliche, anche in ragione della minore attrattività degli impieghi pubblici rispetto al settore privato. Vi è inoltre il problema dei consumi energetici legati ai Data Center.

Diviene allora importante assicurare una adeguata conduzione delle procedure di gara per l'acquisto di IA.

Anzitutto, l'amministrazione deve dotarsi di personale esperto nella Commissione di gara.

In secondo luogo, deve garantire policy corrette di gestione dei dati (compresa evidentemente la delicata questione della protezione dei dati personali), sia nell'ipotesi in cui debba cedere dati pubblici al fornitore per il *fine tuning* del sistema, sia nell'ipotesi in cui il sistema che acquista sia stato addestrato dal fornitore, posto che l'amministrazione deve comunque avere contezza dei dati usati per l'addestramento, la validazione e il testing del sistema, dovendo assicurarne, tra l'altro, la rappresentatività e pertinenza ai sensi del ricordato art. 26 del regolamento UE 2024/1689⁵³.

L'amministrazione che acquisti il sistema sul mercato deve poi porsi il problema delle informazioni che riguardano la specifica applicazione, dato che in quanto soggetto pubblico è tenuto ad assicurare la pubblicità dei sistemi che utilizza nello svolgimento dei propri compiti e la comprensione del loro funzionamento. Ciò sia per ragioni di *accountability* (l'amministrazione risponde del funzionamento dei sistemi di cui si avvale e dei risultati che producono, e deve dunque anzitutto conoscerne gli elementi fondamentali), sia nella relazione con i cittadini, i quali devono poter esercitare, anche nei confronti dell'algoritmo, il diritto di accesso⁵⁴.

Tale esigenza di pubblicità pone il problema della *disponibilità* del codice sorgente: in fase di negoziazione con il fornitore l'amministrazione dovrebbe assicurarsi l'accesso al codice sorgente come opzione preferibile (qualora l'applicazione non sia disponibile in *open source*), soprattutto nel caso in cui il sistema venga usato *per adottare decisioni pubbliche o per determinare elementi sostanziali della decisione*. La possibilità di accedere al codice sorgente è infatti *condizione di legittimità* di una decisione amministrativa che sia

⁵³ V. il paragrafo 3.4 delle linee guida di AgID sul procurement intitolato Ruolo del dato nel procurement.

⁵⁴ Anche su tale profilo, si veda il principio di trasparenza riportato nelle Linee Guida AgID in tema di procurement, secondo cui i requisiti informativi devono assicurare un adeguato livello di visibilità sul funzionamento e tracciabilità del sistema al fine di garantire alla p.a. le informazioni necessarie a comprendere, governare e verificare il funzionamento del sistema lungo tutto il suo ciclo di vita.





presa con un algoritmo o con l'apporto sostanziale di un algoritmo (di recente, il già citato caso BOSCO della Corte Suprema Spagnola e la giurisprudenza del nostro Consiglio di Stato⁵⁵).

Qualora il fornitore non sia disposto a cedere i diritti di privativa, e tale circostanza sia compatibile con quanto previsto in termini di diritto di accesso – si pensi alla necessità di non rendere accessibile il codice sorgente di un algoritmo di analisi del rischio utilizzato dall'agenzia delle entrate per individuare possibili evasori fiscali –, resta comunque ferma la necessità per l'amministrazione di ottenere dal provider informazioni il più possibile complete sui dati di addestramento utilizzati e sulla logica decisoria. Tale condizione è imposta dall'art. 13 del Reg Ue per i sistemi ad alto rischio, ma – per quanto riguarda le amministrazioni italiane – è conseguenza sia dell'art. 30 del codice dei contratti pubblici (d. lgs. 36 del 2023) sia dell'art. 14 della l. 132 del 2025 (l. italiana sull'IA) secondo cui «Le pubbliche amministrazioni utilizzano l'intelligenza artificiale allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati *la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo*»⁵⁶.

Anche nel caso, quindi, di un sistema che compia un compito ancillare o meramente preparatorio, l'amministrazione deve poter assicurarne ai cittadini la conoscenza dei principali elementi, nel rispetto dei principi di pubblicità e di trasparenza dell'azione amministrativa e delle garanzie proprie dello Stato di diritto⁵⁷. In questi termini, anche quando l'accesso al codice sorgente non trova protezione, come è stato di recente per la decisione del nostro Consiglio di Stato 4857/2025 con riguardo ad un software adoperato in una procedura di gara come mero supporto alle attività dell'amministrazione, ciò non dovrebbe sollevare l'amministrazione dall'ottenere (in sede di procurement) – e dal fornire poi agli interessati – le informazioni di base sul ruolo svolto dall'IA nella procedura e sulla sua logica di funzionamento, secondo un approccio sì graduato ma al contempo rispettoso del principio di trasparenza dell'azione pubblica⁵⁸.

Cons. Stato, sez. VI, 4 febbraio 2020 n. 881; Tribunal Supremo, 11 settembre 2025. Sul caso BOSCO sia consentito rinviare a J. PONCE SOLÈ, B. MARCHETTI, *Algoritmi, diritto di accesso e buon andamento. Quale equilibrio? Il caso BOSCO*, in *GDA*, 1/2026, 76.

⁵⁶ In questa stessa direzione vanno le Linee Guida AgID al punto 7.2, che dovrebbero a breve diventare applicabili a tutte le p.a.

⁵⁷ Sull'accessibilità al codice sorgente si veda da ultimo la decisione BOSCO del Tribunal Supremo spagnolo, su cui sia consentito rinviare a B. MARCHETTI, J. PONCE SOLÈ, *Algoritmi, diritto di accesso e buon andamento: quale equilibrio? La sentenza della Corte Suprema spagnola dell'11 settembre 2025 sul caso BOSCO*, in *Giornale di diritto amministrativo*, 1, 2026, 76. Sul rapporto tra pubblicità e accessibilità degli atti amministrativi e proprietà intellettuale v. BLOCH-WEHBA, *Access to Algorithms*, in *Fordham Law Review*, 88(4), 2020, 1265; C. COGLIANESE, D. LEHR, *Transparency and Algorithmic Governance*, in *Administrative Law Review*, 71(7), 2019; A.A. GIKAY, *Trade Secrecy in Automated Decisions. Against the Myth of Irreconcilability and the Imposition of patent*, July 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4861462; M. MAGGIOLINO, *EU Trade Secrets law and Algorithmic Transparency*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3363178. In questi termini, ancora, può richiamarsi l'approccio seguito dal Conseil Constitutionnel francese nel caso *Parcoursup* n. 2020-834 del 3 aprile 2020, secondo cui «Il est loisible au législateur d'apporter à ce droit des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi».

⁵⁸ In questi stessi termini rilevano le Linee Guida AgID sul principio di trasparenza che parlano appunto di proporzionalità tra trasparenza ed efficacia dell'azione amministrativa.



6. Quale coordinamento tra amministrazioni?

Dai dati raccolti è possibile ravvisare che solo sporadicamente – e in riferimento solo ad alcune sperimentazioni delle Regioni (ad esempio riguardanti la razionalizzazione delle liste di attesa in sanità) con la regia di AgID – vi è un'attività di coordinamento dell'azione delle diverse amministrazioni funzionale ad assicurare lo scambio di buone pratiche e il confronto sui problemi comuni.

Sarebbe forse auspicabile, in un momento di grande fermento e sperimentazione, favorire canali di collaborazione e scambio tra le amministrazioni finalizzati a promuovere una programmazione comune e il riuso di applicazioni concepite in *open source* e utilizzabili, a seguito di *fine tuning*, da diverse autorità. In questi termini, anche considerata l'importanza di affiancare le amministrazioni sul piano tecnologico e delle competenze informatiche, sarebbe auspicabile un maggior impegno dei vertici politici in questa direzione, sia in termini di finanziamenti dedicati agli investimenti in IA e tecnologie digitali, sia attraverso un eventuale potenziamento di AgID e di Agenzia per la Cybersecurity sia, ancora, tramite la costituzione di unità specializzate – anche mobili – dedicate allo sviluppo di sistemi di IA per le amministrazioni pubbliche. Ricordiamo che la l. 132/2025, pur prevedendo all'art. 14 comma 3 che «Le pubbliche amministrazioni adottano misure tecniche, organizzative e formative finalizzate a garantire un utilizzo responsabile dell'intelligenza artificiale e a sviluppare le capacità trasversali degli utilizzatori» stabilisce altresì, nel successivo comma 4 che «Le pubbliche amministrazioni provvedono agli adempimenti previsti dal presente articolo con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente».

Analoghe sinergie dovrebbero riguardare anche il momento della formazione dei funzionari e la redazione di linee guida e istruzioni ad essi dedicate per stabilire le modalità di uso dell'IA generativa (anche per evitare il fenomeno della *shadow AI*).

Da un lato, è infatti indubbio che per avere un impiego sapiente di tale tecnologia all'interno delle amministrazioni è fondamentale accrescere le capacità operative dell'amministrazione, dotando i funzionari, attraverso una formazione continua, delle competenze necessarie (non a caso il regolamento europeo include tra i suoi principi la *AI literacy* di *deployer* e *provider*, sebbene il Digital Omnibus on AI ne abbia indebolito la portata) per il controllo e la sorveglianza dei sistemi: tale condizione, come è noto, è ritenuta essenziale sia dal regolamento europeo 2024/1689 che dalla legislazione nazionale, la quale relega l'IA a strumento di supporto, confidando nel «potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale».

Dall'altro, quanto alle linee guida, sarebbe importante che esse muovessero le p.a. non solo a regolare l'uso interno di IA generativa, in ragione dei rischi di allucinazioni e di bias legati a tale tecnologia, insieme con l'*automation bias* (cioè la tendenza a fare eccessivo affidamento nella macchina), ma anche a diffondere la consapevolezza nei funzionari dell'esistenza di specifici costi ambientali connessi all'uso dei LLM (Copilot, Chat GPT, Gemini, Claude ecc.).

7. Un bilancio di luci ed ombre

Le amministrazioni italiane sono ormai avviate sulla strada dell'IA. Molti, come visto, sono i sistemi in fase di sperimentazione e di utilizzo, diversi gli impieghi e le tipologie, e considerevoli gli investimenti finanziari. Alla luce di una tendenza che pare inarrestabile, anche alla luce dei compiti sempre più complessi asse-



gnati alle amministrazioni, uno sguardo di insieme sulle realtà indagate ci consente, tuttavia, di scorgere segnali positivi ma anche elementi critici.

Tra i fattori da guardare con favore vi è la crescente consapevolezza dell'amministrazione in ordine ai rischi che si accompagnano a questa tecnologia, rischi che la differenziano da altre tecnologie fino ad ora utilizzate. Il principale fattore di attenzione, ad oggi, riguarda il trattamento lecito dei dati, che le p.a. hanno chiaro di dover assicurare sia quando sviluppano in house il sistema, sia quando ricorrono al mercato. In proposito, alcune amministrazioni hanno promosso, anche al fine di mantenere i propri dati in un ambiente sicuro, partnership con enti di ricerca e Università o addirittura sviluppato in proprio l'IA.

Altro segnale positivo riguarda la cautela con cui le amministrazioni guardano all'impiego di IA generativa da parte dei propri dipendenti. In generale, è diffusa la consapevolezza di un uso generalizzato e sotto-traccia dei maggiori LLMs (*shadow AI*), con corrispondente preoccupazione sia per le possibili violazioni della privacy, sia per gli errori e le c.d. allucinazioni. Tale preoccupazione ha portato le amministrazioni più solerti (sebbene non ancora in numero significativo) a prevedere già linee guida e raccomandazioni e comunque ad avviare una prima riflessione su usi consentiti o vietati di tali modelli.

In generale, poi, le amministrazioni paiono consapevoli che quanto più l'impiego di sistemi di IA condiziona decisioni con effetti esterni (sui cittadini) tanto più aumentano le criticità. Il risultato è che le p.a. si orientano su applicazioni con finalità conversazionali (chatbot) o comunque preparatorie e di analisi dei dati. Tali scelte sembrano scongiurare – ad oggi – l'uso di IA ML per l'adozione di decisioni o per decidere elementi sostanziali di decisioni aventi effetti esterni e di portata individuale.

Altro elemento positivo che si rinviene riguarda le esigenze di formazione della forza lavoro: è matura la consapevolezza che per poter "governare" l'IA le amministrazioni devono assicurare una formazione continua ai propri dipendenti, al momento sforzati delle competenze trasversali necessarie ad assicurare che l'IA mantenga un ruolo strumentale ed ausiliario rispetto alla persona umana. Su tale aspetto le amministrazioni si stanno attrezzando ma occorrerebbe uno stanziamento di risorse pubbliche aggiuntive per costruire al meglio tali nuove competenze trasversali.

Venendo alle ombre, ciò che sembra di potersi rilevare è che le amministrazioni italiane procedono in ordine sparso. Vi sono realtà molto avanzate – sia quanto a sperimentazione e sistemi impiegati, sia quanto a governance interna, sia quanto a consapevolezza dei problemi da affrontare – e realtà in forte ritardo. L'assenza di un tessuto normativo comune (fino alla recente l. 132/2025 e al regolamento Ue 2024/1689) ha consentito l'avvio di esperienze algoritmiche senza indicazioni vincolanti sulla governance, sui casi d'uso, sulle pratiche da seguire. Ovviamente la presenza di competenze informatiche e di *data analysis* interne (proprie soltanto di alcune autorità di regolazione e di qualche agenzia statale) ha favorito l'automatizzazione dei processi di INPS, Agenzia delle Entrate, Banca d'Italia, Consob, AGCom, mentre i Ministeri, per esempio, non hanno sviluppato analoghe accelerazioni.

Al momento manca una regia comune (perfino, talvolta, all'interno dei singoli Ministeri) e non è ancora affinata, nonostante i lodevoli sforzi di AgID, la condivisione di buone pratiche, di modelli di governance, di strumenti di procurement, di percorsi di formazione del personale. Oltre a ciò, mancano gli investimenti finanziari necessari per attrarre computer scientists nell'amministrazione e per assicurare lo sviluppo di unità tecniche a supporto delle amministrazioni, magari capaci di sviluppare applicazioni di interesse comune a più amministrazioni e ispirate al rispetto dei valori pubblicistici che devono informare l'azione pubblica.

Anche la trasparenza e la pubblicità che devono caratterizzare l'azione amministrativa rischiano di perdersi di fronte all'uso dell'IA: è difficile reperire informazioni sui siti istituzionali delle p.a. e ancora non è del tutto chiara la linea tra ciò che deve essere conoscibile e ciò che può essere legittimamente coperto dai diritti di proprietà intellettuale.

Ed ancora, la consapevolezza dell'esigenza di mantenere i dati in un ambiente sicuro entra in un qualche modo in contraddizione con il diffuso ricorso a soluzioni di mercato non europee.

Infine, la ponderazione dei costi ambientali ed energetici è per ora assente, anche se cresce la presa di coscienza del problema, soprattutto per le amministrazioni che hanno propri data center.

Nel complesso, la messa a punto di nuove regole e prassi adatte alla nuova dimensione algoritmica dell'amministrazione e funzionali a controllarne i rischi sembra appena cominciata. E se le regole giuridiche poste dal regolamento Ue 2024/1689 e dalla l. 132/2025 tracciano senz'altro i binari dentro cui le amministrazioni sono chiamate a muoversi, pare indubbio che il "governo" ottimale di questa tecnologia dipenderà in larga parte dalla capacità delle singole amministrazioni di adottare *buone* decisioni, elaborando buone pratiche e formando adeguatamente i propri dipendenti. Non solo: occorrerà andare oltre le previsioni vincolanti delineate a livello europeo e nazionale anche se si intendono prendere sul serio le ricadute negative dell'IA sull'ambiente in termini di energia, acqua e terre rare.

