Intelligenza artificiale e Pubblica Amministrazione: l'importanza dei *distinguo* per comprendere rischi e opportunità

Barbara Marchetti

Abstract

The paper examines the use of artificial intelligence in the context of administrative action, adopting an approach that distinguishes between different uses of AI technology and various types of artificial intelligence. Depending on the AI system considered, there can be different trade-offs. Systems based on model-based algorithms, for example, allow us to explain how the machine arrives at certain outputs starting from specific inputs. This is not the case with machine learning algorithms, as they cannot be explained in terms of their decision-making logic, making them less compatible with the fundamental principles of administrative action. The paper then explores the topic of European regulation of artificial intelligence, analyzing its key features, and further discusses the need to adequately prepare public officials responsible for overseeing the system (human in the loop) and those in charge of acquiring AI systems.

Das Kapitel untersucht die Anwendung künstlicher Intelligenz (KI) bei öffentlichem Verwaltungshandeln in Italien. Dabei wird sowohl zwischen verschiedenen Einsatzmöglichkeiten von KI-Technologien als auch den unterschiedlichen Ausformungen künstlicher Intelligenz unterschieden. Je nach KI-System ergeben sich unterschiedliche Abwägungen und Kompromisse. Systeme, die auf modellbasierten Algorithmen beruhen, ermöglichen beispielsweise eine Nachvollziehbarkeit, wie die Maschine aus bestimmten Eingaben zu bestimmten Ausgaben gelangt. Dies ist bei maschinellen Lernalgorithmen nicht der Fall, da deren Entscheidungslogik nicht erklärbar ist. Dadurch sind sie weniger kompatibel mit den grundlegenden Prinzipien des Verwaltungshandelns.
Anschließend wird die europäische Regelung von künstlicher Intelligenz beleuchtet sowie deren zentrale Merkmale analysiert. Hervorgehoben wird außerdem die Notwendigkeit, öffentliche Bedienstete angemessen vorzubereiten, wobei der Fokus sowohl auf denjenigen liegt, die für die Überwachung der Systeme verantwortlich sind ("Human in the Loop"), als auch auf jenen, die mit der Beschaffung von KI-Systemen betraut sind.

I. Premessa

Sono state dette molte cose su questa tecnologia dall'impatto trasformativo sulla società, sull'economia e sulle vite di tutti noi:[1] io proverò a calare

1 Si veda *Han*, Infocrazia. Le nostre vite manipolate dalla rete (2023); *Ferrarese*, Poteri nuovi. Privati, penetranti, opachi (2022); *Habermas*, Nuovo mutamento della sfera

queste riflessioni nel mondo dell'amministrazione e della sua attività, e a dedicare di seguito alcune considerazioni al tema della regolazione dell'intelligenza artificiale (IA).[2]

---

pubblica e politica deliberativa, (2023); *Zuboff*, The Age of Surveillance Capitalism (2019); *Casini*, Lo Stato nell'era di Google. Frontiere e sfide globali (2020); *Torchia*, Lo Stato digitale (2023); *Torchia*, Poteri pubblici e poteri privati nel mondo digitale, Il Mulino, Rivista trimestrale di cultura e di politica 1 (2024), 14.

2 *Coglianese*, Administrative Law in the Automated State, Public Law and Legal Theory Research Paper Series, Research Paper No. 21-15, https://scholarship.law.upenn.edu/faculty_scholarship/2273 (22.01.2025); *Coglianese/Lehr*, Regulating by robot: Administrative Decision Making in the Machine Learning Era, Georgetown Law Journal 105 (2017), 1147; *Scherer*, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies and Strategies, Harvard Journal of Law & Technology 29 (2016), 353; *Engstrom et alii*, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies (2020), https://law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf (22.01.2025). Anche la letteratura italiana in tema di IA e diritto (pubblico) è ormai molto vasta. Si vedano, *Avanzini*, Decisioni amministrative e algoritmi informativi. Predeterminazione analisi predittiva e nuove forme di intelleggibilità (2019); *Santosuosso*, Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto (2020); *Pajno et alii*, AI: profili giuridici. Intelligenza artificiale: criticità emergenti e nuove sfide per i giuristi, BioLaw Journal 3 (2019), 205; *Simoncini*, Profili costituzionali della amministrazione algoritmica, Rivista trimestrale di diritto pubblico 4 (2019), 1149; *Auby*, Il diritto amministrativo di fronte alle sfide digitali, Istituzioni del federalismo 3 (2019), 619; *Torchia*, Lo Stato digitale e il diritto amministrativo, in: AA.VV. (Hg), Liber Amicorum per Marco D'Alberti (2022) 477; *Rangone*, Le pubbliche amministrazioni italiane alla prova dell'intelligenza artificiale, in: AA.VV. (Hg), Liber Amicorum per Marco D'Alberti (2022) 494; *Pagano*, Pubblica amministrazione e innovazione tecnologica, relazione al Convegno Associazione Gruppo di Pisa, Genova, 18-19 giugno 2021 su Il diritto costituzionale e le sfide dell'innovazione tecnologica; *Bassini/Liguori/Pollicino*, Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi? in Pizzetti (Hg), Intelligenza artificiale, protezione dei dati personali e regolazione (2018); *Casonato*, Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro, BioLaw Journal, Special Issue 2 (2019), 711; *Casonato*, Intelligenza artificiale e diritto costituzionale: prime considerazioni, Diritto pubblico comparato ed europeo, Special Issue (2019), 101; *Casini*, Lo Stato nell'era di Google. Frontiere e sfide globali (2020); *Marchetti*, La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica, BioLaw Journal 2 (2021), 367; *Costantino*, Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei Big Data, Diritto pubblico I (2019), 43; *Civitarese Matteucci*, Umano, troppo umano. Decisioni amministrative automatizzate e principio di legalità, Diritto pubblico (2019), 5; *Picozza*, Intelligenza artificiale e diritto. Politica, diritto amministrativo and artificial intelligence, Giurisprudenza italiana 7 (2019), 1657; *Donati*, Intelligenza artificiale e giustizia, Rivista AIC 1 (2020), 415; *Simoncini*, L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà, BioLaw Journal 1 (2019), 63; *Armiento*, Pubbliche amministrazioni e intelligenza artificiale. Strumenti, principi e garanzie (2024).

Da quando ho cominciato a studiare questo affascinante argomento non è raro che mi capiti di cambiare idea. In qualche caso i rischi che questa tecnologia presenta mi sembrano, infatti, inaccettabili, mentre in altri casi essi mi paiono trascurabili se rapportati ai vantaggi. Queste oscillazioni tra un approccio distopico ed uno utopistico, tuttavia, non sono il frutto di incoerenza; piuttosto sono indicativi del dilemma che accompagna questa come molte altre innovazioni tecnologiche, in bilico tra la necessità di coglierne le opportunità e l'esigenza altrettanto sentita di contenerne i possibili rischi.

In realtà, più che un approccio basato su una secca alternativa tra IA sì e IA no, si rende necessario un approccio che proceda per *distinguo*, con giudizi e riflessioni che variano a seconda dell'utilizzo che viene fatto dell'IA e a seconda della specifica applicazione di IA impiegata: come vedremo, infatti, cambiano i fattori di rischio e le condizioni di impiego se questa tecnologia viene utilizzata per scopi di ricerca scientifica, o se viene impiegata da un soggetto privato piuttosto che da un soggetto pubblico, o se – in questo ultimo caso – serve per decidere a chi concedere un sussidio o più semplicemente a gestire un *chatbot*[3]. Inoltre, i rischi sono assai diversi se si tratta di IA c.d. *model based*, oppure di IA *Machine learning* (ML) o ancora di IA per finalità generali (*General Purpose AI*).[4]

Vi è poi da considerare un altro fattore rilevante quando ci interroghiamo sui rischi e sui vantaggi legati all'IA: siamo di fronte ad una tecnologia in rapidissima evoluzione. E ciò che in un certo momento può apparirci inconciliabile con una visione antropocentrica dell'intelligenza artificiale, può diventare poi accettabile, sia perché può mutare nel tempo la nostra sensibilità culturale, sia perché possono apparirci assolutamente desiderabili i vantaggi che offre rispetto alle contrindicazioni, sia ancora perché sono stati tecnologicamente superati alcuni dei suoi difetti. Si pensi ad esempio

3 *Glaze/Ho/Ray/Tsang,* Artificial Intelligence for Adjudication: The Social Security Administration and AI Governance, in Bullock et alii (Hg), The Oxford Handbook of AI Governance (2022) 779; *Rachovitsa/Johann*, The Human Rights Implications of the Use of AI inn the Digital Welfare State: Lessons learned from the Dutch SyRI Case, Human Rights Law Review 22 (2022), 1; V. il Rapporto del 2022 della Commissione europea "*Artificial Intelligence in public Services*", https://joinup.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/document/infographic-artificial-intelligence-public-sector (22.01.2025).

4 Per una breve introduzione al tema cfr. *Traverso*, Breve introduzione tecnica all'intelligenza artificiale, DPCE online 51 (2022), 155.

al problema della c.d. *black box* e agli sforzi che i *computer scientists* stanno compiendo per il suo superamento.[5]

Alla luce di tutto questo, è allora consigliabile un approccio metodologico che, lungi dal proporre un lasciapassare incondizionato all'impiego della IA, proceda ad un'analisi caso per caso.

Considerando specificamente l'amministrazione pubblica si potrebbero allora individuare usi dell'intelligenza artificiale che non richiedono la fissazione di particolari limiti, perché presentano molti vantaggi e rischi assai limitati ed altri che invece richiedono regole e cautele particolari o addirittura la previsione di specifici divieti.

Per poter avanzare nella nostra riflessione, occorre però operare anzitutto una distinzione tra tecnologia digitale e IA. Se si parla di tecnologia digitale intesa come dematerializzazione delle attività, ossia come passaggio dall'analogico al digitale, è evidente che in tale accezione, la digitalizzazione ha praticamente solo effetti positivi, operando sul piano dell'efficienza e del buon andamento della Pubblica Amministrazione (d'ora innanzi PA).

Tramite l'utilizzo di tecnologia digitale, i processi decisionali possono essere più celeri e sicuri e l'azione pubblica più trasparente e meno manipolabile; si facilitano le comunicazioni con i cittadini e gli operatori economici; si accelera l'accesso ai documenti; si contrastano eventuali pratiche corruttive. Possono esservi talune criticità, legate al pericolo di esclusione dovuto al *digital divide*, ancora presente nel nostro Paese, ma non paiono esservi rischi specifici sul fronte dei diritti fondamentali e della *rule of law*.

Altra cosa è, invece, l'intelligenza artificiale, perché essa modifica in modo sostanziale *la struttura* del potere, altera il modo in cui le decisioni si formano: e ciò perché una componente di esse o la decisione stessa viene

5 *Longo et alii,* Explainable Artificial Intelligence 2.0 (XAI): A Manifesto of Open Challenges and Interdisciplinary Research Directions, Information Fusion 106 (2024), https://doi.org/10.1016/j.inffus.2024.102301 (22.01.2025); *Xu et alii,* Explainable AI: A Brief Survey on History, Research Areas, Approaches and Challenges, CCF International Conference on Natural Language Processing and Chinese Computing (2019), 563, https://www.researchgate.net/profile/Feiyu-Xu/publication/336131051_Explainable_AI_A_Brief_Survey_on_History_Research_Areas_Approaches_and_Challenges/links/5e2b496f92851c3aadd7bf08/Explainable-AI-A-Brief-Survey-on-History-Research-Areas-Approaches-and-Challenges.pdf (22.01.2025); *Casey/Farhangi/Vogl,* Rethinking Explainable Machines: The GDPR's "right to explanation" Debate and the Rise of Alghorithmic Audits in Enterprise, Berkeley Technology Law Journal 34 (2019), 143; *Pasquale*, The Black Box Society. The Secret Algorithms that Control Money and Information (2016); *Bathaee*, The Artificial Intelligence Black box and the Failure of Intent and Causation, Harvard Journal of Law and Technology 31, 2 (2018), 890.

affidata ad un procedimento algoritmico, e non più solo a funzionari umani, spostando la sede delle scelte, determinando un mutamento delle logiche di fondo e del linguaggio con cui la decisione viene presa, e generando così problemi di comprensibilità e spiegabilità dell'azione amministrativa.[6]

Inoltre, l'algoritmo non è neutro, perché incorpora delle scelte ed esso è sovente fornito da un soggetto privato, il quale non è tenuto ad informare la macchina ai valori o alle finalità che devono orientare le amministrazioni pubbliche, con l'effetto di una potenziale esternalizzazione delle decisioni pubbliche. È dunque evidente che i due fenomeni – del digitale e della decisione algoritmica – disvelano pro e contro assai differenti, e richiedono per tale motivo considerazioni e bilanciamenti di diverso tipo.

II. L'importanza di distinguere tra diversi tipi di IA

Anche parlare genericamente di intelligenza artificiale non basta per la nostra analisi, essendo necessario distinguere tra diversi tipi di applicazioni di intelligenza artificiale poiché ai diversi sistemi corrispondono diversi *trade-off*. Se si parla degli algoritmi deterministici, si parla di sistemi che giungono ai propri *output* sulla base di una logica causale (*if – then*), ovvero, data una certa premessa, si produce sempre la stessa conseguenza, di tipo automatico, e la macchina non fa che elaborare i dati sulla base di regole ed istruzioni predefinite dal programmatore. Il percorso decisorio è ripetibile, spiegabile e ricostruibile a ritroso.

Ciò è rilevante per il nostro discorso su IA e amministrazione pubblica, perché l'uso di questo tipo di algoritmi consente di rispettare, pur con qualche avvertenza (ossia che venga garantito il diritto di accesso al codice sorgente e sia assicurata la traducibilità della regola tecnica in regola giuridica, come ha evidenziato il Consiglio di Stato nella sua giurisprudenza)[7], i principi fondamentali di pubblicità e motivazione delle decisioni pubbli-

6 Sia consentito rinviare a *Marchetti*, Amministrazione digitale, in: Mattarella/Ramajoli (Hg), Funzioni amministrative, Enc. dir., I tematici, III (2022) 75, in cui la distinzione è tra digitalizzazione formale e sostanziale.

7 Si tratta delle decisioni TAR Lazio, Sez III, n 9227/2018, Cons Stato n 881/2020, n 2270/2019 e n 8472/2019, ampiamente annotate dalla dottrina. La giurisprudenza del Consiglio di Stato è stata successivamente recepita nell'art 30 del codice dei contratti pubblici, dedicato all'impiego di IA e *blockchain* nell'attività contrattuale della PA (d lgs n 36/2023). Nella stessa direzione pare ora muoversi il disegno di legge presentato lo scorso aprile recante disposizioni e delega al Governo in materia di intelligenza artificiale.

che. Allo stesso tempo, l'impiego di algoritmi deterministici in procedure standardizzate in cui occorre tenere conto di una grande mole di dati dà vantaggi significativi in termini di correttezza, margini quasi nulli di errore, celerità, sicurezza, efficienza.

Tuttavia, questo tipo di algoritmi non è sempre adatto allo scopo e soprattutto non è performante rispetto ai molteplici compiti che l'amministrazione deve assolvere, per i quali, invece, grande utilità possono avere algoritmi più sofisticati, caratterizzati da apprendimento automatico. A fronte di questo tipo di IA, il *trade off* può essere molto maggiore: essi, infatti, hanno caratteri poco conciliabili con le regole ed i principi che governano l'amministrazione pubblica: sono opachi, hanno rischi elevati di impatto discriminatorio, a causa dei *bias* che possono essere contenuti nei dati, lavorano secondo inferenze statistico-probabilistiche e non causali, e non si prestano ad essere controllabili dal giudice se si traducono in decisioni lesive dei terzi.

Se consideriamo l'impiego di questo tipo di algoritmi in attività di comunicazione (*chatbot*) o per scopi genericamente conoscitivi, il margine di vantaggio appare ancora elevato, e i rischi restano contenuti. Se, invece, il procedimento algoritmico sostituisce del tutto il procedimento amministrativo e va a determinare il contenuto sostanziale di una decisione amministrativa individuale, idonea ad incidere su interessi e diritti dei destinatari, ciò non può non entrare immediatamente in tensione con i valori pubblicistici, in primis pubblicità e trasparenza, diritto alla motivazione, accesso alla tutela giurisdizionale e, non da ultimo, diritti di partecipazione, ossia l'intero nucleo di garanzie fondamentali forgiato dai diritti amministrativi dei Paesi occidentali.

Non stupisce, dunque, che ad oggi, l'uso dell'IA ML in funzione decisoria appaia molto ridotto. Da un'osservazione condotta sulle amministrazioni italiane, si ricava la tendenza ad impiegare IA *machine learning* per svolgere solamente attività preparatoria, volta per lo più a meglio indirizzare le attività di vigilanza delle autorità indipendenti e delle Agenzie statali (ad esempio così è per Banca d'Italia e Consob, per l'Agenzia delle entrate, per l'INPS) o ad estrarre conoscenza dai dati (*data mining*) per orientare le *policies* ambientali, di mobilità urbana, di sicurezza pubblica e così via. Mentre non si hanno, ad oggi, algoritmi *machine learning* che stabiliscano

direttamente chi possa essere ammesso o meno ad una determinata Università oppure chi possa beneficiare o meno di un certo sussidio pubblico.[8]

C'è poi l'ingresso sulla scena della IA Generativa, nota anche come *General Purpose AI (GPAI)*, che abbiamo imparato a conoscere come Chat GPT (ma altre applicazioni sono *Midjourney, Bard, Gemini*). Questa tecnologia pone nuove sfide e rischi inediti. Rispetto alla IA *machine learning* tradizionale è caratterizzata da un maggior grado di imprevedibilità e creatività, dall'utilizzo contestuale di enormi mole di dati in formati diversi e non supervisionati, e da rischi significativi di errore (le c.d. allucinazioni).[9]

È evidente che il suo uso da parte dell'amministrazione pone ulteriori problemi inediti e richiede regole apposite volte ad evitare impatti negativi sull'azione pubblica.

È dunque necessario distinguere tra "cose" e "cose": un conto sono gli algoritmi controllabili, spiegabili, chiamati solo a processare in modo automatico le istruzioni impartite dal funzionario. Un altro conto sono gli algoritmi non spiegabili, che non dovrebbero essere usati per adottare la decisione, ma semmai per fare altre cose, come *chatbot* e assistenti virtuali, o per estrarre conoscenza dai dati.

In mezzo a questi due impieghi, meramente preparatorio e conoscitivo, da un lato, e decisorio in senso proprio, dall'altro, vi è però una situazione intermedia che occorre qui considerare, in cui l'applicazione di IA non sostituisce direttamente il funzionario nell'adozione della decisione, ma si pone come ausilio, limitandosi a suggerire o raccomandare al decisore umano un certo esito.

Da un certo punto di vista, si tratta di una fattispecie meno problematica rispetto al caso in cui la macchina sostituisce il funzionario. Tuttavia, nello stesso tempo, occorre capire quale sia il rapporto tra la raccomandazione che esce dalla macchina e la successiva decisione umana, occorre cioè stabilire se il ruolo dell'IA sia effettivamente solo ausiliario oppure no.

---

8 Cfr. *Chiti/Marchetti/Rangone*, L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali, in: Pajno/Donati/Perrucci (Hg), Intelligenza artificiale e diritto: una rivoluzione? Volume 2, Amministrazione, Responsabilità, giurisdizione (2022).

9 Sulla GPAI v. *Floridi*, AI as agency without intelligence: on ChatGPT, Large Language Models and other generative models, Philos. Technol. 36, 15 (2023); in termini critici sulla disciplina prevista nell'*AI Act* per l'intelligenza artificiale per finalità generali, v. *Novelli et alii*, Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity, Computer Law & Security Review 55 (2024).

È stato, infatti, dimostrato, sulla base di una serie di esperimenti di psicologia comportamentale, che il decisore umano tende a fidarsi molto di quello che la macchina gli dice, tanto da esserne facilmente catturato.

Antoine Garapon ha utilizzato l'espressione effetto *moutonnier* (pecorone) per rendere l'idea della tendenza a fare eccessivo affidamento nella macchina, una sorta di facile scorciatoia che potrebbe sacrificare o annullare l'autonomia del decisore. Il rischio è stato paventato soprattutto con riguardo alla funzione giurisdizionale, poiché si immagina che il giudice, preoccupato di smaltire il lavoro, possa facilmente incorrere in ciò che viene definito, anche dal regolamento europeo sull'IA, *automation bias*, ed ometta così di operare una effettiva sorveglianza umana sul funzionamento del sistema. Ma analoghi rischi valgono per le decisioni amministrative.[10]

È probabilmente questa la sfida più importante che siamo chiamati ad affrontare, quella da cui dipende la capacità di assicurare un uso della tecnologia funzionale all'uomo ed antropocentrica, e si tratta di una sfida particolarmente complessa proprio con riguardo alla amministrazione pubblica. Quest'ultima, infatti, deve poter contare su funzionari adeguatamente preparati, in grado di sapere come funziona la macchina, capaci di interpretare gli *output*, di correggerne gli esiti, e di interromperne il funzionamento quando necessario.

Nell'amministrazione di oggi ci sono competenze digitali, e specifici traguardi in tal senso sono stati indicati anche dal Piano nazionale di ripresa e resilienza (PNRR) ma non c'è ancora una preparazione specifica sull'intelligenza artificiale, non essendosi fatto molto per assicurare quella che il regolamento europeo 2024/1689 in materia di IA chiama, all'art 4, *AI literacy*.

In altri ordinamenti, per esempio negli Stati Uniti, l'alfabetizzazione della forza lavoro in materia di IA è stata importante nell'agenda politica di Biden, che ha promosso l'emanazione nel 2022 dello *AI Training Act* volto ad assicurare che i funzionari pubblici dell'amministrazione federale siano specificamente preparati per affrontare la sfida dell'intelligenza artificiale. Ma anche Regno Unito e Francia si muovono con iniziative simili, se si considera che il Consiglio di Stato francese nel suo studio sull'IA (*Intelligence artificielle et action publique: construire la confiance, servir*

10 *Garapon/Lassegue*, Justice digitale (2018); sia consentito rinviare anche a *Marchetti*, BioLaw Journal 2 (2021), 395.

la performance)[11] ha raccomandato che nei percorsi di formazione per i funzionari pubblici almeno un corso sia dedicato specificamente all'intelligenza artificiale.

III. La regolazione europea dell'IA

Se l'Unione Europea ha da un lato spinto, anche attraverso il *Next Generation EU*, la transizione digitale e con essa lo sviluppo dell'IA, dall'altro, consapevole dei rischi di tale tecnologia, ha, già nel 2021, formulato una proposta di regolamento in materia che è giunta alla sua approvazione definitiva nel luglio del 2024. I tempi di gestazione della regolamentazione ci danno l'idea della difficoltà di regolare questo oggetto: si tratta di una disciplina basata su un approccio proporzionato al rischio che, da un lato, intende tutelare i diritti fondamentali dei cittadini potenzialmente minacciati dall'IA ma, dall'altro, mira a promuovere la ricerca e lo sviluppo in tale settore, allo scopo di attrarre investimenti sul territorio dell'Unione.[12] Il punto di equilibrio tra regole e innovazione è però tutt'altro che facile da trovare, e le ingenti regolazioni approvate per il settore digitale dall'Unione Europea sono sul banco degli imputati, ritenute tra i fattori di freno della competitività europea e di svantaggio dell'Unione nei confronti di Cina e Stati Uniti.[13]

---

11 *Conseil d'Etat*, Intelligence artificielle et action publique : construire la confiance, servir la performance. Etude adoptée en assemblée générale plénière du 31/03/2022, https://la-rem.eu/wp-content/uploads/2023/01/Conseil-dEtat-IA-et-action-publique.pdf (22.01.2025).

12 *Novelli et alii*, AI Risk Assessment: A Scenario-based Proportional Methodology for the AI Act, DISO 3, 13 (2024); *Donati*, Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale, Dir. un. eur. 3-4 (2021), 453. Sia consentito rinviare anche a *Casonato/Marchetti*, Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale, BioLaw Journal 3 (2021), 415; *Marchetti*, La regolazione europea del mercato dell'intelligenza artificiale, Riv. Reg. Mercati 1 (2024), 3.

13 Ritiene che la regolazione non inibisca necessariamente l'innovazione *Bradford*, The False Choice Between Digital Regulation and Innovation, Northwestern University Law Review 118, 2 (2024), 377. Cina e Stati Uniti adottano un approccio regolatorio molto leggero, preoccupati che le regole possano limitare lo sviluppo e la ricerca nel settore. Ciononostante, tra i due Paesi, proprio gli Stati Uniti risultano maggiormente paralizzati, se si esclude l'Order 14110 di Biden, rispetto all'adozione di discipline vincolanti di carattere federale. La Cina, dal 2021 ad oggi ha adottato tre distinte misure, rispettivamente atte a contrastare i deep fake e gli algoritmi di profilazione

Il regolamento trova la sua base normativa nell'art 114 TFUE e stabilisce diversi regimi di circolazione del prodotto IA a seconda del grado di rischio che introduce nel mercato europeo. Alcune applicazioni a rischio inaccettabile vengono vietate ed altre a rischio non elevato o minimo possono circolare liberamente nel mercato, salvi alcuni obblighi di informazione e l'adozione di codici di condotta. La gran parte del regolamento è dedicata ai sistemi ad alto rischio, la cui circolazione nel mercato è condizionata dal rispetto di alcuni requisiti stabiliti negli artt 9-15 del regolamento.

Nella previsione di questi requisiti è evidente la necessità di trovare un compromesso tra esigenze di protezione e sviluppo. Ne è un esempio la disposizione che governa il tema dei dati (art 10), la quale si rivolge a chi intenda immettere nel mercato europeo un sistema di IA ad alto rischio. Essa stabilisce che i dati con cui vengono addestrati tali sistemi debbano essere *sufficientemente* rappresentativi e *per quanto possibile* esenti da errori, completi e pertinenti. È interessante rilevare che nella proposta originaria della Commissione gli avverbi *sufficientemente* e *per quanto possibile* non erano presenti. Tuttavia, il successivo aggiustamento è stato necessario proprio per venire incontro alla esigenza di rendere la norma "tecnologicamente sostenibile", benché così facendo, si sia corrispondentemente diminuita la capacità della stessa di assicurare la qualità dei dati in ingresso (che è fondamentale per garantire la qualità degli *output*) e l'accuratezza del sistema.

Peraltro la stessa rappresentatività dei dati non scongiura di per sé il rischio di esiti discriminatori della macchina, come ha dimostrato il noto caso dell'algoritmo *Compas* (che usava i dati forniti dalle risposte ad un questionario con 137 domande che riguardavano età, occupazione, grado di istruzione, vita sociale e relazionale, uso di droghe, opinioni personali e percorso criminale), che, usato dalle Corti statunitensi per stabilire il rischio di recidiva degli imputati, si è rivelato poi fortemente discriminatorio nei confronti della popolazione nera in ragione dei *bias* presenti nei dati.

---

e da ultimo l'IA generativa. Sulla strategia cinese, v. *Sheehan*, The Foundations of AI Governance in China – Tracing the Roots of China's AI Regulations, Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations?lang=en (22.01.2025). In generale, sui diversi approcci sia consentito rinviare a *Chiti/Marchetti*, Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale, Riv. Reg. Mercati 1 (2020), 29; *Marchetti/Parona*, La regolazione dell'intelligenza artificiale. Stati Uniti e Unione europea alla ricerca di un equilibrio, DPCE online (2022), 236.

Ma la norma che riguarda i dati non è la sola a porre problemi di effettività. Anche le disposizioni che fissano gli obblighi di trasparenza e di informazione in capo al fornitore (art 13) o il diritto alla sorveglianza umana (art 14), pur se condividibili nel loro contenuto e nelle finalità, risultano di difficile applicazione pratica, o comunque pongono un problema di adeguatezza della tutela dei diritti e della sicurezza degli utenti.

Ora, senza eccedere nelle critiche del quadro regolatorio europeo, che anzi va apprezzato soprattutto alla luce del sostanziale immobilismo di Stati Uniti e Cina, tali disposizioni mostrano come regolare l'intelligenza artificiale sia una sfida davvero complessa, per vincere la quale potranno essere necessari aggiustamenti futuri del testo e l'adozione di *standards* tecnici e linee guida in grado di aggiornare e sintonizzare le norme rispetto all'evoluzione tecnologica.

Ultimo aspetto della regolazione europea che vorrei toccare in questo breve intervento riguarda, poi, la sua applicazione soggettiva. Come è noto, il regolamento si applica tanto ai fornitori dei sistemi di IA, su cui ricadono molti degli obblighi stabiliti nel regolamento, sia agli utilizzatori (*deployer*), senza che rilevi in modo decisivo la loro natura pubblica o privata. Benché, infatti, il testo abbia conosciuto nel corso dell'iter di approvazione talune modifiche significative che hanno via via previsto alcune norme specificamente dedicate alle pubbliche amministrazioni, l'impianto complessivo del regolamento tratta fornitori pubblici e privati e utilizzatori pubblici e privati sostanzialmente nello stesso modo.

Questa parificazione è interessante nella logica della distinzione pubblico e privato propria anche del nostro ordinamento. Siamo, infatti, abituati a ritenere che le amministrazioni siano soggette a regole diverse da quelle a cui sono soggetti gli attori privati.

Nel sistema disegnato dall'*AI Act*, invece, l'amministrazione che autoproduce o utilizza un sistema ad alto rischio (e sono tali i sistemi che operano nei settori contemplati dall'allegato III, impiegati cioè nell'ambito di servizi pubblici quale l'istruzione, nella giustizia, nell'immigrazione, e nei procedimenti elettorali, ad esempio) deve – al pari dei soggetti privati – garantire che il sistema di intelligenza artificiale risponda a determinati requisiti (menzionati sopra) relativi ai dati, alla sorveglianza umana, agli obblighi di informazione e di trasparenza, che in qualche modo vengono così a sostituire i tradizionali parametri di legalità dell'azione amministrativa.

A fronte di tale sostituzione, tuttavia, occorre chiedersi se il livello di garanzia garantito dal rispetto di tali requisiti sia equivalente a quello assicurato dai tradizionali principi dell'azione amministrativa. Ad esempio,

bisogna domandarsi se un'autorità che adotti la sua decisione servendosi di un algoritmo soddisfi l'obbligo di motivazione previsto dall'art 3 della legge 241/90 limitandosi a spiegare – come impone l'art 86 del regolamento – il ruolo svolto dalla macchina nel procedimento e la logica di fondo del sistema di IA. Occorre insomma chiedersi se dare conto delle banche dati utilizzate per addestrare l'algoritmo e spiegare la logica di fondo dell'algoritmo – posto che, in ragione della *black box,* non è comunque dato sapere la ragione per cui, dati certi *input*, la macchina ha prodotto certi *output* – sia sufficiente per assicurare il diritto di difesa del cittadino cui è preordinato l'obbligo di motivazione posto in capo alla PA.

È, infatti, cosa diversa avere informazioni sul funzionamento del sistema e conoscere le ragioni concrete della decisione con cui si viene, ad esempio, esclusi dal godimento di un sussidio.

Da questo punto di vista, l'*AI Act* pone delle sfide molto interessanti anche per gli Stati. Ad esempio in Germania, per espressa disposizione della legge sul procedimento amministrativo, il sistema di intelligenza artificiale può essere usato solo per adottare decisioni vincolate,[14] limitazione non prevista nel regolamento europeo, il quale prevede, per esempio, chel'IA possa essere utilizzata anche per assistere la PA nell'esercizio di poteri discrezionali.

IV. L'importanza della formazione specifica dei funzionari pubblici

Un ultimo punto riguarda il tema della formazione. Su questo aspetto esiste, come detto, una disposizione specifica nel regolamento europeo, collocata all'inizio del testo, che espressamente stabilisce che i fornitori e gli utilizzatori dei sistemi di IA devono adottare misure atte a garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione nonché il contesto in cui i sistemi di IA devono essere impiega-

14 Per l'ordinamento tedesco, rileva l'art. 35 della legge sul procedimento amministrativo (VwVfG), su cui v. *Buoso*, Fully automated administrative Acts in the German Legal System, ERDAL 1, 1-2 (2020), 113; *Fraenkel-Haeberle*, Fully digitalized Administrative Procedure in the German Legal System, ERDAL 1, 1-2 (2020), 106; la decisione del *Conseil Constitutionnel* francese è invece la n. 765/2018.

ti, e le persone o i gruppi di persone su cui i sistemi di IA devono essere utilizzati (art 4).

La ragione di tale disposizione, che pure esige solo una "alfabetizzazione sufficiente" – e dunque non particolarmente elevata – è evidente: l'IA va governata e le amministrazioni pubbliche, al pari di ogni altro soggetto, non possono essere esentate da tale obbligazione quando usano applicazioni di IA per svolgere i loro compiti ed esercitare i loro poteri. Ciò è fondamentale se si vuole evitare che le applicazioni – e coloro che le sviluppano – sostituiscano i funzionari, con ricadute in termini di *accountability* e di perdita di umanità.

Si è già accennato al fatto che molti Paesi si stanno muovendo nel senso appunto di promuovere una formazione specialistica dei dipendenti pubblici. Tale formazione è importante soprattutto in capo a quei funzionari che sono specificamente chiamati a utilizzare l'IA e a condurre le procedure per l'acquisto della tecnologia.

Con riguardo a tale secondo aspetto, il *Conseil d'Etat* francese, nel rapporto sopra citato su *Intelligence artificielle et action publique*, considera cruciale il momento in cui l'amministrazione acquista il sistema (dato che poche sono le amministrazioni in grado di produrlo *in house*) perché la decisione con cui si sceglie una applicazione di IA è particolarmente delicata: da un lato, nella procedura di gara occorre scongiurare il rischio di asimmetrie informative (tra amministrazione e *provider* privato), ciò che implica adeguate conoscenze specialistiche in capo alla parte pubblica che negozia il contratto; dall'altro, ci sono rischi legati alla sicurezza e alla privacy dei dati, in ragione sia della eventualità di uno scambio di dati (di natura pubblica) necessario per poter addestrare e testare il sistema realizzato dal provider privato, sia per la necessità per l'amministrazione pubblica di conoscere i dati che sono stati utilizzati dal fornitore (nel caso opposto in cui la società che ha sviluppato il sistema si sia avvalsa di altri dati) per l'addestramento, in ragione degli obblighi previsti in capo al *deployer* dall'art 26 del regolamento europeo.

Ciò rende il momento dell'acquisto del sistema di intelligenza artificiale un'occasione importante per adottare le misure volte ad assicurare il buon funzionamento del sistema, vincolare il *provider* al rispetto di specifiche obbligazioni sul trattamento dei dati, richiedere la necessaria attività di assistenza per tutto il ciclo di vita dei contratti e regolare eventuali profili di responsabilità. Non è pensabile che in questa fase la controparte pubblica non sia rappresentata da personale con la necessaria *expertise* tecnica.

V. IA e amministrazione: una sfida complessa

Per le considerazioni sopra esposte, auspicherei un atteggiamento di "apertura con cautela" per l'uso di intelligenza artificiale nella sfera pubblica. Mi pare difficile pensare che l'amministrazione non si debba avvalere di applicazioni che possono aumentare la propria capacità amministrativa, ad esempio, indirizzando l'attività di vigilanza o migliorando la conoscenza dei fatti su cui l'amministrazione va ad operare. Tuttavia, occorre accogliere tale tecnologia con tre avvertenze: prima di tutto, vanno salvaguardate le garanzie del cittadino di fronte al potere. L'uso di algoritmi non deve erodere i diritti a conoscere le decisioni e le ragioni per cui sono prese, né può compromettere il diritto ad una tutela giurisdizionale effettiva. Fintanto che gli algoritmi di apprendimento automatico non sono spiegabili, non possono costituire la decisione che entra in diretta collisione con i diritti del cittadino, pena l'azzeramento di tutte e tre queste garanzie.

In secondo luogo, l'amministrazione deve fornire adeguate informazioni sull'uso che fa dei sistemi di IA, spiegare quale ruolo svolgono nella propria azione amministrativa e con quali effetti, indicare quali dati vengono utilizzati per addestrare gli algoritmi. Deve trattarsi di un'informazione comprensibile anche ai non esperti e facilmente rinvenibile sui siti istituzionali delle amministrazioni e nelle sezioni espressamente dedicate ai singoli procedimenti in cui sono in uso.

Infine, l'uso da parte della PA di tali applicazioni impone una formazione adeguata non solo dei funzionari chiamati ad utilizzare tali sistemi, ma anche di quelli chiamati a guidare le procedure di acquisto. Si tratta di una condizione necessaria per assicurare l'*accountability* dell'azione pubblica e la sorveglianza umana sui processi automatizzati.