RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0117 • articolo sottoposto a peer review • pubblicato in anteprima il 23 nov. 2023

Mauro Barberio

L'uso dell'intelligenza artificiale nell'art. 30 del d.lgs. 36/2023 alla prova dell'AI Act dell'Unione europea*

Il presente lavoro, in prossimità della pubblicazione dell'AI Act dell'Unione europea, mette in relazione l'innovativa (per il sistema giuridico italiano) applicazione dell'intelligenza artificiale al campo dei pubblici appalti – così come dispone l'art. 30 del d.lgs. 36/2023 – con gli istituti di matrice eurounitaria che stanno per vedere la luce. Effettuata una breve introduzione sui sistemi di intelligenza artificiale utilizzabili nel settore in esame, lo scritto si sofferma, *in primis,* sulla problematica qualificazione dell'ambito dei pubblici appalti come attività ad alto rischio, ai sensi e per gli effetti dell'Allegato III dell'AI Act. Viene, altresì, messo in evidenza su chi debba gravare, e da chi debba provenire, quel "contributo umano" che l'art. 30 del d.lgs. 36/2023 stabilisce come inderogabile ai fini della legittimità dei provvedimenti automatizzati nel settore dei pubblici appalti e le ripercussioni che determina, in tal senso, l'individuazione dell'"operatore", pubblico e privato, quale figura chiave e giuridicamente responsabile della sorveglianza umana. Il lavoro si chiude soffermandosi sui sistemi di governance e di prevenzione dei rischi, così come impostati dal legislatore europeo, con particolare riferimento agli istituti di cui alla valutazione d'impatto e alla sperimentazione normativa.

Intelligenza artificiale – Appalti pubblici – Controllo umano – Governance e sperimentazione normativa

The Use of artificial intelligence in Article 30 of Legislative Decree 36/2023 to the test of the EU AI Act

The present work, in close to the publication of the AI Act of the European Union, relates the innovative (for the Italian legal system) application of artificial intelligence to the field of public procurement – as provided for in Article 30 of Legislative Decree 36/2023 – with the EU institutions that are about to see the light of day. With a brief introduction to the artificial intelligence systems that can be used in the sector in question, the paper focuses, first of all, on the problematic qualification of the field of public procurement as a high-risk activity, pursuant to and for the effects of Annex III of the AI Act. It is also highlighted who should burden, and from whom should come, that 'human contribution' that Article 30 of Legislative Decree 36/2023 establishes as mandatory for the purposes of the legitimacy of automated measures in the field of public procurement and the repercussions that determine, in this sense, the identification of the 'operator', public and private, as a key figure and legally responsible for human surveillance. The work ends by focusing on the governance and risk prevention systems, as set by the European legislator, with particular reference to impact assessment and regulatory testing.

Artificial intelligence – Public procurement – Human control – Governance and regulatory testing

L'Autore è avvocato amministrativista abilitato presso le magistrature superiori

* Relazione tenuta al Convegno di studi presso l'Università degli Studi di Cagliari "L'intelligenza artificiale nel diritto amministrativo", 27 ottobre 2023.

1. L'art. 30 del Codice dei contratti pubblici e l'automazione delle attività amministrative

L'art. 30 del nuovo Codice dei contratti rappresenta una novità assoluta nello scenario normativo nazionale in quanto, come noto, ha introdotto e incentivato l'automazione delle attività amministrative nel ciclo di vita dei contratti pubblici, quindi dalla programmazione sino alla fase di esecuzione.

Contestualmente il legislatore ha cercato di calibrare alcuni contrappesi miranti, principalmente, a far sì che le logiche di funzionamento delle soluzioni tecnologiche prescelte potessero essere, non solo, adeguatamente comprese e accessibili, ma anche non esclusivamente riferibili alla macchina. Imponendo che la decisione algoritmica, all'interno del processo decisionale, possa, quindi, essere controllata, validata o smentita dal controllo(re) umano, anche attraverso l'adozione di «ogni misura tecnica e organizzativa atta a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori».

Uno dei primi problemi da porsi, almeno così sembra a chi scrive, è quello teso all'individuazione dell'ambito entro cui, relativamente agli appalti pubblici, potrebbe risultare più funzionale e aderente l'uso dell'intelligenza artificiale. La risposta non risulta particolarmente complicata: si tratta, in tutta evidenza, della fase istruttoria e, quindi, in modo precipuo, della fase di valutazione delle offerte e, precisamente, di quelle tecniche. In quanto le offerte economiche sono già da tempo oggetto di formule (in verità piuttosto essenziali) alfa numeriche che non necessitano dell'intelligenza artificiale per essere sviluppate e controllate.

Non sembra, in effetti, esservi altro ambito, all'interno del procedimento di gara (se non forse quello legato all'eventuale fase di verifica dell'anomalia), maggiormente dedicato per l'applicazione dell'intelligenza artificiale

Dati i presupposti della disposizione codicistica, e ferme le prime analisi effettuate dalla dottrina in merito agli aspetti chiaroscurali della predetta disciplina normativa[1], risulta, in questa sede, di peculiare interesse comprendere quali possano essere le relazioni intercorrenti tra l'art. 30

1. Cfr. Gallone 2023 e, sia consentito, Barberio 2023. Cfr. anche Simoncini 2019; Amato Mangiameli 2022; Taddei Elmi 2021.

del d.lgs. 31 marzo 2023, n. 36 e il nuovo regolamento eurounitario, AI Act (che risulta in fase di approvazione[2]).

Definite le fasi procedimentali di carattere valutativo-decisionale, votate, precipuamente, all'uso dell'intelligenza artificiale, diviene conseguente comprendere quale specifica tipologia di IA possa essere maggiormente aderente alle necessità delle stazioni appaltanti. Tutto ciò anche a voler tralasciare l'aspetto – tutt'altro che irrilevante o, ancor meno, scontato ma non decisivo nella presente analisi – se si possa, o meno, procedere, mediante i provvedimenti automatizzati, a effettuare scelte discrezionali o se questi debbano essere, esclusivamente, destinati per dinamiche procedimentali vincolate[3].

Lo strumento automatizzato più funzionale per un'eventuale comparazione delle offerte tecniche è certamente quello proprio delle tecnologie di cui ai modelli linguistici di grandi dimensioni (tradotto dall'acronimo LLMs – *Large Language Models*), cui appartengono quei sistemi che si basano su degli *input* sorgenti (prompt) che poi, conseguentemente, generano e restituiscono una sequenza di parole, codici o dati (output). I sistemi più recenti di LLMs includono GPT-3, PaLM, LaMDA, Gopher and OPT[4].

Questi modelli hanno una capacità straordinaria di rispondere alle sollecitazioni che vengono loro proposte – tanto con riferimento alla qualità del riscontro quanto all'immediatezza della risposta – ma, per poter essere adeguatamente consultati e ottenere esiti conferenti ed efficaci, necessitano di due indefettibili presupposti che ne rendano sostenibili gli esiti (output, ossia "previsioni, raccomandazioni o decisioni che rispondono agli obbiettivi del sistema sulla base degli input provenienti da tale ambiente") o che ne possano consentire, altrimenti, il loro rigetto attraverso un'istruttoria che possa portare alla loro smentita[5].

2. La disciplina eurounitaria tra *data training* e governance

I due presupposti per una corretta ed efficace applicabilità alle regole dell'evidenza pubblica delle dinamiche proprie dei LLMs si fondano, da un lato, su un sistema di addestramento (training) che dovrà essere adeguato alla specifica attività istruttoria che verrà effettuata. D'altro lato sarà necessario impostare e garantire un rigoroso sistema di controlli (governance) da porre in essere tanto a posteriori quanto, però, anche a priori[6], al fine di controllare, verificare ed, eventualmente, smentire la decisione automatizzata.

Con riferimento al primo problema e alla necessità di un adeguato addestramento del sistema di intelligenza artificiale, non sembra inutilmente ozioso far rilevare come i predetti sistemi LLMs rispondono alle sollecitazioni proposte (tramite

2. «The Council agreed the EU Member States' general position in December 2021. Parliament voted on its position in June 2023. EU lawmakers are now starting negotiations to finalise the new legislation, with substantial amendments to the Commission's proposal including revising the definition of AI systems, broadening the list of prohibited AI systems, and imposing obligations on general purpose AI and generative AI models such as ChatGPT», European Parliament (*Artificial Intelligence Act*).
3. Lo scontro interpretativo, in merito a questa problematica, è già in essere all'interno della giustizia amministrativa tra le sentenze n. 2270, sez. VI, dell'8 aprile 2019 («la discrezionalità amministrativa …non può essere demandata al software, è quindi da rintracciarsi al momento dell'elaborazione dello strumento digitale») e n. 8472, sez. VI, del 13 dicembre 2019 che, invece, facendo leva su una, per la verità discutibile, contestazione «a monte dell'attualità di una tale distinzione» (tra attività amministrativa vincolata piuttosto che discrezionale, n.d.a.), ammette che «se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità».
4. Mokander-Schuett-Kirk-Floridi 2023; Floridi-Chiriatti 2020; Charlotin 2023.
5. Art. 30 co. 3 lett. b «non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata».
6. Una corretta governance dovrebbe occuparsi, con particolare attenzione, anche della fase anteriore non tanto e non solo per la verifica dell'addestramento della macchina (training) ma anche per prevenire distorsioni ed errori assieme alla chiara definizione delle regole e modalità di interventi correttivi.

input) tanto proattivamente quanto più hanno sviluppato, mediante adeguato training, le proprie conoscenze e abilità all'interno di sistemi adeguati di apprendimento automatico (*machine learning*), anche attraverso un sistema di apprendimento profondo (*deep learning*) tramite reti neurali.

È agevolmente rilevabile (e di questo si dovrà, necessariamente, tenere conto), infatti, come i sistemi di IA abbiano possibilità di funzionamento attraverso «livelli di autonomia variabili, il che significa che dispongono almeno di un certo grado di autonomia di azione rispetto ai controlli umani e di capacità di funzionare senza l'intervento umano» (considerando n. 6 AI Act dell'Ue). Quel grado di autonomia variabile, che può arrivare a essere anche assoluto, si sviluppa, però, all'interno di un ambiente (che è il contesto entro cui operano i sistemi automatizzati) che è condizionato dagli input forniti, da ciò che è già ivi presente e, poi, successivamente, lo sarà pure dagli stessi output creati dal sistema che, quindi, lo implementano e alimentano («Tale output influenza ulteriormente detto ambiente anche solo mediante l'introduzione di nuove informazioni» – cons. n. 6). In questi termini appare evidente che gli esiti che vengono sollecitati al sistema di intelligenza artificiale sono condizionati grandemente dall'ambiente entro cui il medesimo pasce e si nutre.

La prima sfida, pertanto – anche a livello di governance "preventiva" – sarà quella di garantire (e verificare) che il sistema si sia sviluppato in un ambiente adeguato con riferimento al preteso risultato da raggiungere. Ambiente di addestramento del sistema automatizzato che, evidentemente, condizionerà il livello qualitativo dell'esito atteso. Appare pertinente far rilevare, infatti, come (anche in termini di prevenzione di eventuali risposte discriminatorie o per evitare la decantazione di *bias*) la criticità si ravvisi e si possa sviluppare, non tanto e non solo, nella tipologia di algoritmo utilizzato, quanto piuttosto nell'ambiente e nei dati (*data training*) attraverso i quali il sistema è stato, o si è, autonomamente, addestrato.

Se non vi saranno set di dati adeguati, qualitativamente e quantitativamente, il risultato che la macchina restituirà sarà parziale, limitato, errato o qualitativamente insufficiente.

Il legislatore eurounitario ha chiara questa problematica e la espone, in maniera efficacissima, nei considerando nn. 42, 43 e 44 («Un accesso ai dati di alta qualità svolge un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessaria l'attuazione di adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento e, ove applicabile, di convalida e prova, incluse le etichette, dovrebbero essere sufficientemente pertinenti, rappresentativi, adeguatamente verificati in termini di errori e il più possibile completi alla luce della finalità prevista del sistema. Dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato, prestando particolare attenzione all'attenuazione di possibili distorsioni nei set di dati, che potrebbero comportare rischi per i diritti fondamentali o risultati discriminatori per le persone interessate dal sistema di IA ad alto rischio. Le distorsioni possono ad esempio essere intrinseche agli insiemi di dati di base, specie se si utilizzano dati storici, inseriti dagli sviluppatori degli algoritmi o generati quando i sistemi sono attuati in contesti reali. I risultati forniti dai sistemi di IA sono influenzati da tali distorsioni intrinseche, che sono destinate ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti … I requisiti relativi alla governance dei dati possono essere soddisfatti ricorrendo a terzi che offrono servizi di conformità certificati, compresa la verifica della governance dei dati, dell'integrità dei set di dati e delle pratiche di addestramento, convalida e prova dei dati»).

Dovrebbe, quindi, essere garantito (anche a livello di specifiche tecniche di cui all'art. 79 e all'All. II.5 del d.lgs. 36/2023) – prima di essere utilizzato in determinate gare e per valutare le conseguenti offerte tecniche – che il sistema di intelligenza artificiale sia certificato per aver operato all'interno di specifici ambienti e con set di dati pertinenti e adeguatamente rappresentativi. Non può che essere questo il senso di quanto dispone l'art. 16.1 a-*quater* dell'AI Act che impone, per i sistemi di IA ad alto rischio, che siano fornite «le specifiche per i dati di input o qualsiasi altra informazione

pertinente in termini di set di dati utilizzati, compresi i relativi limiti e le relative ipotesi, tenendo conto della finalità prevista e degli usi impropri prevedibili e ragionevolmente prevedibili del sistema di IA».

3. Tra apprendimento supervisionato e *deep learning*

Alla luce di queste prime, essenzialissime, considerazioni sembra potersi affermare come, all'interno del quadro stabilito dall'art. 30 del Codice dei contratti pubblici, il più sicuro e affidabile sistema di intelligenza artificiale, per quanto quivi di interesse, risulti essere quello con apprendimento supervisionato. In quanto si manifesta come lo strumento che può rispondere, in maniera più efficace, alle condizioni ivi stabilite dal legislatore che, non a caso, impone una supervisione effettiva, attraverso un efficace contributo umano che possa essere "capace di controllare, validare ovvero smentire la decisione automatizzata". Sistema che, peraltro, quando non li elimina, riduce notevolmente output complessi e opachi che ne rendono difficile la comprensibilità e, quindi, anche la possibilità di esplicazione degli esiti[7]. Il legislatore europeo ha ben chiaro il rischio della predetta deriva e, infatti, per quelle attività c.d. "ad alto rischio"[8] impone, all'art. 14.1, sistemi di intelligenza artificiale con apprendimento supervisionato: «I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da essere efficacemente supervisionati da persone fisiche in misura proporzionale ai rischi associati a tali sistemi».

Viene, insomma, sostanzialmente, posto il veto – per le attività ad alto rischio – per quei sistemi di intelligenza artificiale con capacità di apprendimento profondo (c.d *deep learning*) senza supporto umano. Questa modalità di apprendimento, infatti, non prevede alcun intervento umano che possa suggerire le risposte possibili o intervenire in via diretta, in quanto «deve essere messa in condizione di sbagliare un numero così elevato di

7. AI Act, considerando 6-*bis:* «La funzione e gli output di molti di questi sistemi di IA si basano su relazioni matematiche astratte che per gli esseri umani risultano difficili da comprendere e monitorare e i cui input specifici sono difficili da rintracciare. Tali caratteristiche complesse e opache (elemento "scatola nera") incidono sulla rendicontabilità e sulla spiegabilità».

8. AI Act, art. 6 – *Regole di classificazione per i sistemi di IA ad alto rischio*: «A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza ai sensi della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi in relazione ai rischi per la salute e la sicurezza ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II. 2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio i sistemi di IA che rientrano in uno o più settori critici e casi d'uso di cui all'allegato III, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche. Qualora un sistema di IA rientri nell'allegato III, punto 2, è considerato ad alto rischio se presenta un rischio significativo di danno per l'ambiente. Sei mesi prima dell'entrata in vigore del presente regolamento, la Commissione, previa consultazione dell'ufficio per l'IA e dei pertinenti portatori di interessi, fornisce orientamenti che specificano chiaramente le circostanze in cui l'output dei sistemi di IA di cui all'allegato III comporterebbe un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche o i casi in cui non lo farebbe». Per l'All. III: «I sistemi di IA di cui ai punti da 1 a 8-*bis* rappresentano casi d'uso critici e sono tutti considerati sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, a condizione che soddisfino i criteri di cui a tale articolo: 1) Sistemi biometrici e basati su elementi biometrici. …2. Gestione e funzionamento delle infrastrutture critiche. …3. Istruzione e formazione professionale. …4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo. …5. Accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi. …6. Attività di contrasto. …7. Gestione della migrazione, dell'asilo e del controllo delle frontiere. …8. Amministrazione della giustizia e processi democratici»; Mollicone 2023.

volte da individuare l'errore e provvedere in autonomia a correggere la propria sequenza»[9].

4. Attività ad alto rischio e appalti pubblici: quale relazione

La domanda è, a questo punto, obbligata: il settore dei pubblici appalti rientra o meno all'interno delle attività ad alto rischio?

La risposta a questo interrogativo dovrebbe essere verosimilmente negativa qualora ci si fermasse all'analisi specifica del settore e, quindi, sulla base di una verifica strutturale della disposizione normativa. Giusto quanto fa rilevare l'AI Act (all'art. 6 e nell'Allegato III), gli appalti pubblici non sono, infatti, qualificabili *ex se* come un ambito predicabile quale settore ad alto rischio.

A fronte, però, di una verifica sostanziale e in concreto, dell'operato che la stazione appaltante porrà effettivamente in essere, non sarebbe agevole riuscire ad estromettere la singola procedura di gara da una possibile classificazione come attività qualificabile ad alto rischio. Tanto nel caso in cui l'appalto dovesse ricadere, specificamente, in uno di quegli ambiti predeterminati dal legislatore eurounitario come settore ad alto rischio, in forza di una correlazione che non sembra possa essere troppo rarefatta (basti pensare agli ambiti della "gestione e funzionamento delle infrastrutture critiche", dell'"accesso a prestazioni e servizi pubblici e a servizi privati essenziali" o della "gestione e funzionamento della fornitura di acqua, gas, riscaldamento, energia elettrica e infrastrutture digitali critiche"). Così come non sembra potersi escludere, in termini più generali, come ad alto rischio quell'attività valutativa intrinseca, sui fatti e/o disposizioni normative, qualora effettuata da un'amministrazione, o da un organo amministrativo, attraverso sistemi di intelligenza artificiale[10].

Restano, comunque, da considerare due aspetti, sui quali è necessario, seppur *en passant*, porre l'accento, in merito alla sufficienza e rilevanza del concetto di alto rischio in materia di pubblici contratti. Da un lato appare illusorio pretendere di incasellare, in modo determinato e preventivo, la fenomenologia di tutti rischi – non solo futuri, ma pure quelli presenti, alti o bassi che possano essere ritenuti – e i loro correlativi ambiti, a fronte dell'imprevedibilità e liquidità della materia[11]. D'altro canto chi scrive aderisce a quella tesi che

9. Pesucci 2022; cfr. ancora Lo Sapio 2021: «I sistemi di Deep Learning utilizzano un'architettura di modelli matematici ispirata alle reti neurali biologiche: le cd. reti neurali artificiali. Tale modello è costituito da un gruppo di interconnessioni di informazioni (si parla infatti di approccio di "connessionismo" al calcolo, contrapposto all'approccio simbolista): gli input trasmettono i segnali, ad una potenza ovviamente incomparabile con quella dei neuroni biologici, ai diversi nodi che costituiscono una rete complessa (deep) e nel corso dell'apprendimento, i "pesi" di ciascun nodo vengono continuamente riparametrati, in un percorso non lineare e multistrato la cui ricostruzione però sfugge alla comprensione umana».

10. Il considerando 40 recita, in modo non inequivocabile, «È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o da un organo amministrativo, o per loro conto, per assistere le autorità giudiziarie o gli organi amministrativi nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie» e, pure, l'Allegato III, punto 8, lett. a, fa rilevare come siano ad alto rischio: «i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o da un organo amministrativo, o per loro conto, per assistere un'autorità giudiziaria o un organo amministrativo nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti o utilizzati in modo analogo nella risoluzione alternativa delle controversie».

11. «AI harms are very different in different contexts, where they might be already addressed by particular sectoral laws. At the same time, most AI harms can readily be traced to a pattern of similar problems. Problems of incomplete or biased training data ("garbage in, garbage out") and poorly designed human machine systems (including ignoring known cognitive biases and overreliance on a human in the loop) resonate across sectors», Kaminski 2022. «Moreover, given the multiplicity and complexity of the ethical and social risks associated with LLMs, we anticipate that policy responses will need to be multifaceted and incorporate several complementary governance mechanisms. As of now, technology providers and policymakers have only started experimenting with different governance mechanisms, and how LLMs should be governed remains an open question», Mokander-Schuett-Kirk-Floridi 2023; Engler 2023.

qualifica, di per sé stesse, rischiose – non tanto l'ambito di utilizzazione quanto piuttosto – l'applicazione e l'utilizzazione concrete dei sistemi generativi di intelligenza artificiale[12].

Ferme le predette valutazioni, il primo presupposto per un'adeguata e legittima utilizzazione dell'intelligenza artificiale, nei procedimenti di gara, sarà quello di avere un sistema supervisionato che sia stato addestrato in un ambiente adeguato affinché possa restituire output che siano i più conferenti, logici e corretti possibili e che possano essere controllati, verificati e, nell'eventualità, anche smentiti da un sorvegliante umano che disponga di «un livello sufficiente di alfabetizzazione in materia di IA conformemente all'articolo 4-*ter* nonché del sostegno e dell'autorità necessari per esercitare tale funzione, durante il periodo in cui il sistema di IA è in uso e per consentire indagini approfondite a seguito di un incidente» (art. 14.1 AI Act).

5. Contributo umano e responsabilità dell'"operatore" privato e pubblico

La declinazione necessitata di questo, primo, presupposto ci conduce all'interrogativo in ordine a quale debba essere il contributo umano preteso per giungere, eventualmente, anche alla smentita della decisione automatizzata, ai sensi della lett. b) del co. 3 dell'art. 30 del Codice dei contratti pubblici che, come noto, impone la non esclusività della decisione algoritmica.

L'intero AI Act dell'Ue è, peraltro, pervaso dalla necessità dell'intervento umano o, meglio, della "sorveglianza umana"[13], finalizzata a evitare e correggere le, sempre, possibili distorsioni sistemiche e per far sì che vengano «adottate misure tecniche e organizzative per garantire che i sistemi di IA ad alto rischio siano quanto più possibile resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi» (art. 15.3 AI Act).

La cattiva notizia – se così la si può definire – che determinerà, a parere di chi scrive, la fuga delle stazioni appaltanti dall'auspicato (da parte del legislatore del d.lgs. 36/2023) uso delle procedure automatizzate, trae la propria ragion d'essere dal tarlo che si insinua in conseguenza del considerando n. 58-*bis* che responsabilizza, in maniera massiva, gli "operatori"[14], i quali, ai sensi dell'art. 3.4, vengono individuati in

12. «The alternative scenario would be that all generative AI systems would fall under the high risk category because it cannot be excluded that they may be used also in a high-risk area. In that case, there may be a serious risk of over-regulation. For this reason, rather than trying to fit general-purpose AI systems into existing high-risk categories, we propose that they should be considered a general-risk category in their own right, similar to the way that chatbots and deep fakes are considered a separate risk category of their own, and subject to legal obligations and requirements that fit their characteristics», Helberger-Diakopoulos 2023.

13. Cfr. considerando nn. 1, 4-*bis*, 9-*bis*, 43 e l'art. 4-*bis*. Tra gli altri si segnalano poi gli artt. 7 e 14 anche se, in effetti, il richiamo alla possibilità di «di intervenire sul funzionamento del sistema di IA ad alto rischio o di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga, che consenta di arrestare il sistema in condizioni di sicurezza» appare piuttosto *naif*.

14. Considerando 58-*bis*: «Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche dal modo in cui tali sistemi di IA sono utilizzati. Gli operatori di sistemi di IA ad alto rischio svolgono pertanto un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA. Gli operatori sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi emarginati e vulnerabili. Gli operatori dovrebbero individuare strutture di governance adeguate in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana, le procedure di gestione dei reclami e le procedure di ricorso, dal momento che le scelte relative alle strutture di governance possono essere determinanti per attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Al fine di garantire in maniera efficiente la tutela dei diritti fondamentali, l'operatore di sistemi di IA ad alto rischio dovrebbe quindi effettuare una valutazione d'impatto sui diritti fondamentali prima di metterli in servizio. La valutazione d'impatto dovrebbe essere corredata di un piano dettagliato che descriva le misure o gli strumenti che contribu-

«qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

Il pericolo dell'intelligenza artificiale viene, quindi, normativamente collegato non tanto alla sua materiale produzione e messa in commercio, bensì, massimamente, al suo concreto utilizzo. Il rischio viene riconnesso all'immanenza del suo uso e, pertanto, viene scaricato sull'operatore che viene individuato come responsabile e come destinatario di una notevole messe di obblighi[15], tra i quali, per quanto in questa sede rileva, brilla il dovere di sovrintendenza umana sulle attività automatizzate («Nella misura in cui esercitano un controllo sul sistema di IA ad alto rischio, gli operatori: i) attuano la sorveglianza umana conformemente ai requisiti stabiliti nel presente regolamento; ii) garantiscono che le persone fisiche preposte ad assicurare la sorveglianza umana dei sistemi di IA ad alto rischio siano competenti, adeguatamente qualificate e formate e dispongano delle risorse necessarie per assicurare l'efficace supervisione del sistema di IA a norma dell'articolo 14; iii) garantiscono che le misure pertinenti e adeguate in materia di robustezza e cibersicurezza siano periodicamente monitorate per verificarne l'efficacia e siano periodicamente adeguate o aggiornate» – art. 29.1-*bis*).

Ulteriore interrogativo è quello di stabilire se la sorveglianza umana, il controllo umano o la riserva di umanità, comunque la si voglia definire, sia derogabile o, meglio, se sia giuridicamente disponibile da parte del privato, eventualmente sollecitato in merito da un'amministrazione che intenda procedere, per esempio, attraverso sistemi di intelligenza artificiale non supervisionati e, quindi, non governati da successiva sorveglianza umana. Se vi sia, insomma, la possibilità di prestare consenso a un'attività esclusivamente automatizzata senza possibilità che venga controllata, validata o smentita. In termini generali, dal lato squisitamente normativo, in forza del regolamento Ue 679/2016 – richiamato copiosamente dall'AI Act e ritenuto trasversalmente applicabile alla disciplina *de qua* – nulla sembra ostarvi. Il citato regolamento ammette, infatti, espressamente la disponibilità del consenso, in siffatte ipotesi, ai sensi dell'art. 22: «1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: …c) si basi sul consenso esplicito dell'interessato»[16].

iranno ad attenuare i rischi per i diritti fondamentali individuati al più tardi a partire dal momento della loro messa in servizio. Se tale piano non può essere individuato, l'operatore dovrebbe astenersi dal mettere in servizio il sistema. Nell'effettuare tale valutazione d'impatto, l'operatore dovrebbe informare l'autorità nazionale di controllo e, nella misura più ampia possibile, i pertinenti portatori di interessi nonché i rappresentanti dei gruppi di persone che potrebbero essere interessati dal sistema di IA al fine di raccogliere le informazioni pertinenti ritenute necessarie per effettuare la valutazione d'impatto e sono incoraggiati a rendere pubblica la sintesi della loro valutazione d'impatto sui diritti fondamentali sul loro sito web online. Tali obblighi non dovrebbero applicarsi alle PMI che, data la mancanza di risorse, potrebbero incontrare difficoltà nello svolgimento di tale consultazione. Tuttavia, esse dovrebbero altresì adoperarsi per coinvolgere tali rappresentanti nello svolgimento della loro valutazione d'impatto sui diritti fondamentali. Inoltre, dati il potenziale impatto e la necessità di sorveglianza e controllo democratici, gli operatori di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione, nonché gli operatori che sono imprese designate come gatekeeper a norma del regolamento (UE) 2022/1925, dovrebbero essere tenuti a registrare l'uso di qualsiasi sistema di IA ad alto rischio in una banca dati pubblica. La registrazione è possibile, su base volontaria, anche per altri operatori».

15. Cfr. artt. 23, 27, 28, 29, 51, 62.

16. «Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito"» – Garante della privacy, "Principi fondamentali del trattamento". Si richiama, però, una recente sentenza della Corte di cassazione che prescrive un percorso, per il rilascio del consenso, più articolato a garanzia del privato: «Il problema, per la liceità del trattamento, era invece (ed è) costituito dalla validità – per l'appunto – del consenso che si assume prestato al momento dell'adesione. E non può logicamente affermarsi che l'adesione a una piattaforma da parte

La ricaduta pratica del consenso all'eventuale disumanizzazione del procedimento (e quindi del conseguente provvedimento) automatizzato non potrebbe mai essere la, ipoteticamente, sperata emarginazione e deresponsabilizzazione dell'umano, in quanto il nostro sistema costituzionale impone che sia l'uomo e non la macchina a rispondere delle proprie azioni[17].

6. La valutazione d'impatto come strumento principale di governance e suoi limiti

Un adeguato sistema di governance rappresenta il secondo pilastro per la migliore, e legittima, utilizzazione, nel campo dei pubblici appalti (ma non solo, ovviamente), dei sistemi di intelligenza artificiale.

Nonostante vi sia chi propone sistemi di governance complessi e differentemente articolati[18], chi scrive ritiene di aderire all'impostazione fornita da alcuni studiosi statunitensi che hanno evidenziato la specificità e l'assoluta novità della sfida lanciata dall'intelligenza artificiale che impone risposte totalmente nuove e altre[19] rispetto a una concezione, di controllo e verifica, che potrebbe essere definita tradizionale.

La legislazione europea sta sviluppando il proprio indirizzo sulla governance cercando di trovare delle linee di azione innovative e coraggiose sulle quali – in un quadro liquido quale quello in esame – saranno il tempo e l'esperienza a darci risposte in merito alla loro efficacia e, quindi, alla necessità di eventuali, quanto probabili, correzioni.

Così come la responsabilità, anche la gestione della governance, viene delegata agli operatori che, ai sensi del considerando 58-*bis*, dovrebbero «individuare strutture di governance adeguate in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana, le procedure di gestione dei reclami e le procedure di ricorso, dal momento che le scelte relative alle strutture di governance possono essere determinanti per attenuare i rischi per i diritti fondamentali in casi d'uso concreti») e determinare – a priori e qualora si rientri «in uno o più settori critici e casi d'uso di cui all'Allegato III» (ved. art. 6.2 AI Act) – una modalità preventiva di valutazione tesa a qualificare/quantificare l'impatto del sistema di intelligenza artificiale, redigendo un "piano dettagliato" che descriva, tra l'altro, le misure e gli strumenti finalizzati all'attenuazione dei rischi e che raccolga le informazioni pertinenti ritenute necessarie per effettuare l'indicata valutazione.

Il predetto istituto (*rectius* la valutazione di impatto[20]) conosce in ambito europeo la propria

dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi riconoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati», Corte di cassazione, sez. I civ, n. 14381 del 25 maggio 2021.

17. «La mancanza di effettivo contributo umano determinerebbe evidenti questioni di legittimità costituzionale in relazione alla violazione degli artt. 28, 97 co. 3 e 98 che valorizzano le funzioni e le responsabilità dei pubblici dipendenti o in relazione alla violazione dell'art. 54 co. 2 che riconnette le funzioni pubbliche alla persona fisica (anche perché sulla base delle, tuttora insuperate, leggi di Isaac Asimov sulla robotica, il robot non può essere chiamato a responsabilità)» Barberio 2023; Gallone 2023.

18. «Our findings most directly concern technology providers as they are primarily responsible for ensuring that LLMs are legal, ethical, and technically robust. Such providers have moral and material reasons to subject themselves to independent audits, including the need to manage financial and legal risks and build an attractive brand». Si tratta di un approccio innovativo quanto distonico rispetto a quello eurounitario che responsabilizza, non tanto i fornitori o i produttori quanto, come sopra fatto rilevare, massimamente, gli operatori. Mokander-Schuett-Kirk-Floridi 2023.

19. «AI cannot be governed like any previous technology, and it is already shifting traditional notions of geopolitical power … the challenge is clear: to design a new governance framework fit for this unique technology. If global governance of IA is to become possible, the international system must move past traditional conceptions of sovereignty and welcome technology companies to the table». Bremmer-Suleyman 2023.

20. Art. 29-*bis* AI Act: «Prima di mettere in servizio un sistema di IA ad alto rischio quale definito all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA destinati ad essere utilizzati nel settore 2 dell'allegato III, gli operatori effettuano una valutazione dell'impatto dei sistemi nel contesto specifico di impiego …».

applicazione in settori particolarmente sensibili quali quello ambientale[21] e quello della tutela dei dati personali[22]. La valutazione di impatto è stata pensata, anche all'interno dell'AI Act, quale strumento necessario per la regolazione specifica dell'intelligenza artificiale nelle ipotesi ad alto rischio e per minimizzarne gli effetti e le possibili ricadute negative.

Si tratta di un sistema di governance teso a individuare, preventivamente, i rischi e a descrivere le misure e gli strumenti finalizzati alla riduzione, ove possibile, di ogni eventuale conseguenza negativa cagionabile dal sistema di IA. Qualora, peraltro, per qualche ragione, non dovesse essere possibile redigere un piano dettagliato ai sensi dell'art. 29-*bis*: «l'operatore si astiene dal mettere in servizio il sistema di IA ad alto rischio e informa senza indebito ritardo il fornitore e l'autorità nazionale di controllo. Le autorità nazionali di controllo, a norma degli articoli 65 e 67, tengono conto di tali informazioni quando conducono indagini sui sistemi che presentano un rischio a livello nazionale».

Il legislatore eurounitario indica quei contenuti generali che la valutazione di impatto deve, necessariamente, contenere, ai sensi dell'art. 29-*bis* dell'AI Act, ossia: «a) una chiara descrizione della finalità prevista per la quale verrà utilizzato il sistema; b) una chiara descrizione dell'ambito geografico e temporale previsto per l'uso del sistema; c) le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema; d) la verifica che l'uso del sistema è conforme al diritto dell'Unione e nazionale in materia di diritti fondamentali; e) l'impatto ragionevolmente prevedibile sui diritti fondamentali di mettere in servizio il sistema di IA ad alto rischio; f) determinati rischi di danno suscettibili di incidere sulle persone emarginate e sui gruppi vulnerabili; g) l'impatto negativo ragionevolmente prevedibile dell'utilizzo del sistema sull'ambiente; h) un piano dettagliato su come saranno attenuati i danni o l'impatto negativo sui diritti fondamentali individuati; j) il sistema di governance che sarà messo in atto dall'operatore, compresa la supervisione umana, la gestione dei reclami e i mezzi di soccorso».

La critica che si ritiene di muovere alla disciplina normativa testé richiamata va individuata nel fatto che la stessa si concentra, quasi totalmente, sul rischio di derive discriminatorie e violazioni di diritti individuali, ma non sembra curarsi a sufficienza della restituzione (negli ambiti pubblicistici e istituzionali) di dati erronei, imprecisi o parziali. Si ritiene, pertanto, che, nella misura in cui un sistema di IA intervenga in una procedura di affidamento, qualificabile come ad alto rischio, alla luce della clausola residuale di cui all'art. 29-*bis* («Tale valutazione comprende, *almeno*[23], i seguenti elementi»), la valutazione di impatto possa essere adeguatamente implementata dall'operatore, in sede di analisi dei possibili e specifici impatti, con contenuti ulteriori e atipici tesi alla migliore efficacia e calibrazione del sistema di intelligenza artificiale.

7. La sperimentazione normativa: un'occasione da non perdere

Una novità che potrebbe risultare utilissima (per sviluppare analisi e dinamiche innovative, di carattere sperimentale, anche nell'ambito dei pubblici appalti e, comunque, dei procedimenti amministrativi) è quella che, ai sensi dell'art. 53 dell'AI Act, consente degli spazi di sperimentazione normativa per l'IA («1. Gli Stati membri istituiscono almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in applicazione del presente regolamento. Tale spazio di sperimentazione può anche essere istituito congiuntamente con uno o diversi altri Stati membri. 1-*bis*. Possono essere istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale o congiuntamente con altri Stati membri … 1-*quater*. Le autorità costituenti assegnano risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva. 1 quinquies. Gli spazi di sperimentazione normativa per l'IA, conformemente ai criteri di cui all'articolo 53-*bis*, garantiscono un ambiente controllato che promuove l'innovazione e facilita

21. Direttiva 85/337/CEE del 27 giugno 1985.

22. Art. 35 del regolamento Ue 2016/679 del 27 aprile 2016.

23. Corsivo aggiunto.

lo sviluppo, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico concordato tra i potenziali fornitori e l'autorità costituente; 1-*sexies*. L'istituzione di spazi di sperimentazione normativa per l'IA è intesa a contribuire ai seguenti obiettivi: a) le autorità competenti forniscano orientamenti ai potenziali fornitori di sistemi di IA per conseguire la conformità normativa con il presente regolamento o, se del caso, ad altre pertinenti normative applicabili dell'Unione e degli Stati membri; b) i potenziali fornitori consentano e agevolino la sperimentazione e lo sviluppo di soluzioni innovative relative ai sistemi di IA; c) apprendimento normativo in un ambiente controllato».

Si tratta di un'occasione irripetibile che il legislatore nazionale (così come per quelli regionali più dinamici e propositivi) non dovrebbe perdere e attivare ben prima dell'entrata in vigore del regolamento comunitario[24] per portarsi avanti nell'applicazione pratica e sperimentale dell'intelligenza artificiale nella sua relazione con l'amministrazione pubblica. Questa concessione normativa consente di calibrare, anche per "lotti" o "stati di avanzamento", l'efficacia dell'intelligenza artificiale in ambiti specifici e di testarne l'efficacia, senza la pretesa di definire, da subito, un sistema normativo compiuto che rischierebbe di essere o troppo acerbo o, altrimenti, di nascere già superato.

Quale migliore applicazione, per la sperimentazione normativa, potrebbe esserci rispetto a quella degli appalti pubblici che hanno già la porta spalancata, all'utilizzazione dell'intelligenza artificiale, dall'art. 30 del d.lgs. 36/2023?

Riferimenti bibliografici

A.C. Amato Mangiameli (2022), *Intelligenza artificiale, big data e nuovi diritti*, in "Rivista italiana di informatica e diritto", 2022, n. 1

M. Barberio (2023), *L'utilizzo degli algoritmi e l'intelligenza artificiale tra futuro prossimo e incertezza applicativa*, giugno 2023

I. Bremmer, M. Suleyman (2023), *The AI Power Paradox. Can States Learn to Govern Artificial Intelligence — Before It's Too Late?*, in "Foreign Affairs", September/October 2023

D. Charlotin (2023), *Large Language Models and the Future of Law*, August 2023

A. Engler (2023), *Early thoughts on regulating generative AI like chatgpt*, February 2023

L. Floridi, M. Chiriatti (2020), *GPT-3: Its nature, scope, limits and consequences*, in "Mind and Machine", vol. 30, 2020, n. 4

G. Gallone (2023), *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Cedam, 2023

N. Helberger, N. Diakopoulos (2023), *ChatGPT and the AI Act*, in "Internet Policy Review", vol. 12, 2023, n. 1

M.E. Kaminski (2022), *Regulating the Risks of AI*, August 2022

G. Lo Sapio (2021), *La black box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*", in "federalismi.it", 2021, n. 16

J. Mokander, J. Schuett, H.R. Kirk, L. Floridi (2023), *Auditing large language models: a three-layered approach*, in "AI & Ethics", 2023

24. È consentito, infatti, che detta sperimentazione sia avviata anche prima dell'entrata in vigore del regolamento AI Act, art. 53.1: «Gli Stati membri istituiscono almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in applicazione del presente regolamento».

M.M. Mollicone (2023), *Il rischio dell'intelligenza artificiale applicata. Modelli di allocazione a confronto*, in "Actualidad Jurídica Iberoamericana", 2023, n. 18

S. Pesucci (2022), *Diritto e intelligenza artificiale: opportunità e dilemmi nell'era della automazione*, in "Ristrutturazioni Aziendali", marzo 2022

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "Rivista di BioDiritto", 2019, n. 1

G. Taddei Elmi (2021), *Il Quid, il Quomodo e il Quid iuris dell'IA. Una riflessione a partire dal volume "Diritto e tecnologie informatiche"*, in "Rivista italiana di informatica e diritto", 2021, n. 2