

Legalità, algoritmi e corruzione: le tecniche di intelligenza artificiale potrebbero essere utilizzate *nel e per* il sistema di prevenzione della corruzione?

Francesco Merenda

L'articolo vuole ragionare su quali potrebbero essere i vantaggi e i rischi legati all'impiego delle tecniche di intelligenza artificiale (IA) nel sistema italiano della prevenzione della corruzione. In particolare, ci si sofferma sul processo di gestione del rischio, quale momento cruciale per l'adozione delle misure amministrative di prevenzione della corruzione. L'utilizzo di tecniche IA potrebbe, infatti, perfezionare queste fasi, velocizzare la procedura e garantire maggiore imparzialità nella scelta delle misure. Al contempo però l'adozione di tecniche IA, parziali o totali, porterebbe con sé sia alcuni aspetti problematici sia un significativo ridimensionamento del sistema vigente. Una seconda riflessione è dedicata a quei settori o strumenti che, sebbene non siano da reputare strettamente interni al sistema della prevenzione, potrebbero contribuire alla causa preventiva stessa. Nella parte finale si ragiona sulle conseguenze più difficili che l'applicazione dell'intelligenza artificiale nel campo della prevenzione potrebbe comportare in termini di partecipazione e legalità.

Intelligenza artificiale – Prevenzione della corruzione – Legalità – Partecipazione

SOMMARIO: *Premessa – 1. I motivi che legittimano il ricorso all'IA nel sistema dell'anticorruzione italiano – 2. Campi e strumenti che potrebbero avvalersi dell'IA per il sistema di prevenzione – 2.1. Le procedure di reclutamento del personale della PA – 2.2. Perfezionamento degli indici red flags – 2.3. Investimento nel cd. e-procurement per prevenire ed individuare la corruzione negli appalti pubblici – 2.4. Utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di whistleblowing – 3. Alcune esperienze concrete di applicazione IA nel campo anticorruzione a livello globale – 4. Quali sfide e rischi ne derivano in termini di legalità e partecipazione? – 4.1. Segue. Prevenzione della corruzione e partecipazione – 5. Riflessioni conclusive*

Premessa

È ormai appurato che la pubblica amministrazione si doterà sempre di più di tecniche e strumenti basati sugli algoritmi e, di conseguenza, ci si interroga, in particolare, se l'intelligenza artificiale verrà ampiamente sfruttata anche nel campo della prevenzione della corruzione.

Questo scenario è stato ipotizzato da alcuni studiosi¹ in quanto, attraverso la sostituzione della decisione

umana con quella della macchina, si potrebbe garantire un maggior rispetto del principio d'imparzialità e della legalità stessa. Anche gli organismi internazionali, negli ultimissimi anni, hanno raccomandato sempre di più l'utilizzo di nuovi approcci basati sui dati per migliorare la valutazione del rischio di corruzione² nel settore pubblico.

Partendo da una definizione standard di intelligenza artificiale come quell'insieme di tecnologie in

F. Merenda è dottorando di ricerca in "Legalità, Culture politiche e Democrazia" presso il Dipartimento di Scienze politiche dell'Università degli studi di Perugia. Questo saggio fa parte della sezione monografica *Gli algoritmi pubblici tra legalità e partecipazione* a cura di Benedetto Ponti.



cui le macchine imitano l'intelligenza umana per risolvere problemi complessi, sorgono spontanee alcune domande: i problemi legati alla scarsa effettività delle misure anticorruzione sono da reputare complessi? E ancora, l'impiego esteso delle tecniche IA nella definizione delle misure del Piano triennale di prevenzione della corruzione e della trasparenza (di seguito Ptpct) e di altre azioni preventive potrebbe diventare una componente stabile di quella che sarà la cd. "amministrazione intelligente"³?

1. I motivi che legittimano il ricorso all'IA nel sistema dell'anticorruzione italiano

Occorre, in via preliminare, affermare che la risposta alla domanda che funge da titolo del presente lavoro è affermativa, in quanto questa frontiera è già stata sperimentata in alcuni ordinamenti giuridici. È alquanto interessante invece capire in che modo ciò si potrebbe applicare e se ci saranno concreti progressi per il sistema preventivo della corruzione italiano. Appare dunque ragionevole chiedersi, soprattutto attraverso una prospettiva giuridica, quali sarebbero gli eventuali benefici e problemi derivanti dall'utilizzo di queste tecnologie.

Sono essenzialmente tre le principali cause che giustificano l'impiego delle tecniche di intelligenza artificiale in questo campo: a) l'insufficienza e i limiti dell'attuale sistema dell'anticorruzione italiano; b) i miglioramenti in termini di imparzialità; c) l'efficientamento e la semplificazione delle procedure di approvazione dei Ptpct.

Il sistema di prevenzione amministrativa della corruzione⁴ pone una riflessione sull'effettività delle misure adottate per questa politica, anche alla luce dell'imminente ricorrenza del primo decennio dall'entrata in vigore della legge anticorruzione n. 190/2012. È dunque, oggi, possibile trarre un bilancio dell'impatto prodotto da questa policy, mettendo in rilievo luci e ombre derivanti dalla prassi applicativa delle pubbliche amministrazioni.

Il framework dell'anticorruzione è basato su un impianto "centro-periferico", dove gli indirizzi vengono emanati dall'autorità nazionale anticorruzione e l'attuazione è affidata alle singole amministrazioni, secondo una logica *bottom-up*; l'implementazione del sistema invece poggia su due principali pilastri, che sono i Ptpct e i doveri di comportamento: i primi consistono in una serie di misure *ad hoc* adottate dalle pubbliche amministrazioni dopo un processo preliminare di analisi del rischio e in base al piano nazionale anticorruzione (Pna); le regole di condotta, invece, so-

no sancite nei codici di comportamento dei dipendenti pubblici, oltre a quelle previste da alcune leggi.

Sin dalla prima esperienza applicativa sono emerse alcune criticità di quest'impianto relativamente ad alcuni fattori: le misure dei Ptpct spesso vengono adottate con approccio "adempimentale" quindi non risultano in linea con l'obiettivo di analisi e gestione del rischio; le regole sancite nei codici di comportamento, che dovrebbero introdurre doveri integrativi e coerenti con il tipo di amministrazione, sono il risultato di un puro esercizio esteriore; la formazione, che è un fattore centrale⁵, sollecitato a livello internazionale, ha assunto la forma e la sostanza di meri momenti ritualistici e dunque improduttivi nella prospettiva di creazione e diffusione di una cultura dell'integrità e dell'anticorruzione; ultimo ma non meno importante, il nostro sistema anticorruzione continua a mostrarsi non del tutto in linea con il concetto di integrità pubblica raccomandato dall'Ocse⁶, il quale si basa su un approccio che vede nelle politiche anticorruzione una componente centrale, ma che va necessariamente coadiuvata con altre politiche nel settore pubblico: la promozione dell'efficienza amministrativa e il raggiungimento dei risultati; la diffusione di un settore pubblico professionale e fondato sul merito; incoraggiare una cultura organizzativa aperta; investire in una leadership etica e diffondere una cultura dell'integrità.

Quale IA⁷ per l'ambito di prevenzione? L'intelligenza artificiale si distingue in due macro-tipologie: l'*artificial general intelligence* (AGI) e l'*artificial narrow intelligence* (ANI). La prima è stata definita come «una macchina e o un sistema che può eseguire solo un compito strettamente definito o un piccolo insieme di compiti correlati»⁸; la seconda invece come «una macchina in grado di comprendere il mondo come qualsiasi essere umano e con la stessa capacità di imparare a svolgere un'enorme gamma di compiti»⁹.

Nel caso in questione, ma ad oggi in generale nella maggioranza dei campi, quando si parla di utilizzare queste tecniche ci si riferisce principalmente all'AGI, la quale a sua volta è composta da due categorie principali di programmazione: *rule-based programming* e il *machine learning*¹⁰. La prima forma di programmazione si basa su un processo secondo il quale i programmatori umani scrivono un codice che stabilisce le regole che definiscono tutti gli aspetti di una determinata attività (per es. se succede il fenomeno β , allora ne consegue una specifica risposta δ , se si verifica una situazione diversa da β , allora ne consegue γ). La seconda forma è costituita da macchine che non dipendono dai dati, bensì imparano dai dati e dall'esperienza, un sottocampo di questa forma di programmazione è il cd. *deep learning* formato da modelli di apprendimento automatico detti reti neurali¹¹.



In merito alla seconda tipologia di programmazione si nutrono maggiori perplessità e osservazioni critiche: sebbene siano più veloci ed accurate, l'opacità interna al funzionamento di questi dispositivi non permetterebbe di rendere trasparenti e spiegabili i passaggi che partono dalle premesse e arrivano ai risultati¹².

Le prime esperienze di applicazione dell'IA quindi si inseriscono nel campo dell'*artificial general intelligence*, sebbene vi siano casi¹³ in cui si utilizzano sia la programmazione *rule-based programming* che quella *machine learning*.

La *conditio sine qua non* perché si possa arrivare a buone decisioni automatizzate nel campo della prevenzione della corruzione è ovviamente legato all'uso dei big data¹⁴, consistente in un numero infinito di informazioni e dati. Si può dire infatti che gli algoritmi senza dati sono vuoti e i dati senza algoritmi sono ciechi¹⁵. L'utilizzo dei big data servirebbe quindi per fare scelte più efficienti e intelligenti nel rispetto del principio di legalità¹⁶. Ciò però dovrebbe essere sviluppato in concomitanza con una pubblica amministrazione che sia sempre più digitale e, quindi, soltanto dopo aver superato l'attuale *digital gap*¹⁷. Tale divario è amplificato dalle poche risorse impiegate finora per studiare in modo approfondito l'IA, soprattutto in termini di ricerca e sviluppo¹⁸. Il raggiungimento di questi obiettivi, pertanto, è imprescindibile affinché si possano adoperare strumenti e modelli IA.

Il binomio intelligenza artificiale-big data potrebbe rappresentare il miglior utilizzo delle ICT nel campo dell'anticorruzione: con l'ausilio del *machine learning* e del *deep learning* si potranno fare analisi di dati molto precise fino a permettere l'individuazione di correlazioni e anomalie all'interno di vasti *dataset*.

Prima di ipotizzare quali potrebbero essere gli ambiti ad avvantaggiarsi dell'IA è bene ragionare anzitutto sui potenziali effetti positivi in termini di imparzialità ed efficienza della pubblica amministrazione (di seguito anche PA).

L'impiego di algoritmi predittivi potrebbe favorire il modello di legalità efficiente della PA all'interno del processo di adozione dei Ptpct?

Per quanto concerne il principio di imparzialità, *prima facie*, la risposta immediata non potrebbe che essere positiva. La cd. "decisione robotica" garantirebbe maggiore imparzialità nella scelta rispetto a quella umana che peraltro per sua natura potrebbe essere influenzata¹⁹ e che spesso non tiene in considerazione che la scelta è una responsabilità²⁰. L'automatizzazione e la spersonalizzazione delle scelte eliminano i rischi umani e i cattivi comportamenti dei funzionari e ciò rappresenterebbe una valida garanzia per la prevenzione della corruzione.

Nel processo di definizione delle misure e nella fase preliminare di analisi del rischio dei Ptpct l'IA potrebbe facilitare l'individuazione delle misure che l'amministrazione adotterà al fine di incentivare le buone condotte del personale, assicurando di conseguenza una maggiore imparzialità nelle scelte fatte.

Il Codice dell'amministrazione digitale italiano (d.lgs. 7 marzo 2005, n. 82), precisamente al comma 1 dell'art. 12, afferma che le pubbliche amministrazioni utilizzano le ICT per la realizzazione degli obiettivi di imparzialità, ma anche quelli di efficienza, efficacia, economicità, trasparenza, semplificazione e partecipazione²¹.

Si deve però precisare che l'imparzialità di cui si parla è da circoscrivere alla sola fase di predisposizione delle misure organizzative dei piani di prevenzione. Garantito ciò, però, l'imparzialità soggettiva dei funzionari, quale pietra angolare del sistema di prevenzione italiano, continuerebbe a dipendere dalle condotte di chi lavora alle dipendenze della PA. Tale precisazione è necessaria per sottolineare che, anche se le ipotesi in discussione si dovessero concretizzare, la responsabilità del rispetto delle misure e dei doveri, ma anche di efficacia del sistema complessivo, rimane affidata al personale dell'amministrazione.

Oltre all'imparzialità, potrebbero trarre beneficio dall'applicazione di tecniche di IA anche l'attuazione del principio di buon andamento e i suoi corollari.

Già il Consiglio di Stato nel 2019²² ha affermato che l'utilizzo di siffatte tecniche è conforme con i canoni di efficienza ed economicità dell'azione amministrativa, in particolare grazie: «alla notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o peggio dolo) del funzionario (essere umano) e la conseguente maggior garanzia di imparzialità della decisione automatizzata».

2. Campi e strumenti che potrebbero avvalersi dell'IA per il sistema di prevenzione

Osservando l'iter delle varie fasi dell'adozione dei Ptpct ci si rende facilmente conto che le risorse impiegate sono tante e il personale coinvolto detiene diversi compiti e responsabilità. Ogni attore coinvolto, inoltre, dispone di dati utili e rilevanti che debbono essere forniti con tempestività al Responsabile della prevenzione (Rpct). Già in questa fase, quindi, le risorse di vario tipo potrebbero essere risparmiate, le tempistiche drasticamente ridotte e la gestione dei dati migliorata attraverso l'utilizzo delle tecniche *blockchain*²³.



Si tratta di registri distribuiti che permettono di gestire e aggiornare un registro di dati e informazioni in modalità aperta, condivisa e distribuita senza un controllo centrale e di verifica. In questo modo, oltre ai vantaggi appena detti, si garantirebbe di conseguenza una più rapida e proficua analisi del contesto interno ed esterno. I registri distribuiti permetterebbero quindi una migliore gestione delle fonti dei dati per l'analisi di contesto²⁴, incidendo in positivo sia sull'individuazione e la mappatura dei processi che sull'identificazione di quei dati che potrebbero contenere le caratteristiche organizzative capaci di avere influenza sul profilo di rischio dell'amministrazione.

Un altro significativo apporto dell'IA potrebbe consistere nella possibilità di perfezionare e rendere più attendibili gli indicatori di monitoraggio e anche i cd. *key risk indicators*, utili a fornire indicazioni sul livello di esposizione al rischio del processo o delle sue attività componenti. La definizione di questi indicatori è preliminare al processo vero e proprio: grazie ai dati raccolti in precedenza, l'IA e il *machine learning* riuscirebbero ad elaborare più rapidamente gli indicatori, che sarebbero più precisi ed efficaci.

Inoltre, l'IA potrebbe essere assunta come nuova tecnica per l'individuazione degli eventi corruttivi che si basano su analisi di documenti e banche dati. Ciò consentirebbe una più rapida ed attendibile identificazione e formalizzazione dei rischi, utili per la creazione del "registro degli eventi rischiosi" nel quale per ogni processo si deve individuare almeno un rischio. Le tecniche algoritmiche potrebbero garantire maggiore analiticità e far corrispondere meglio i rischi alle varie fasi del processo. Tuttavia, bisogna considerare che, se da un lato le procedure automatizzate garantirebbero maggiore rapidità e analiticità, dall'altro non sarebbero però capaci di descrivere gli eventi rischiosi che, ad oggi, è un tratto peculiare del processo di costruzione del registro stesso.

Un ultimo contributo, ma forse il più determinante, potrebbe essere quello nella fase di scelta dell'approccio valutativo (qualitativo, quantitativo o misto). Ad oggi, l'ANAC consiglia²⁵ la scelta di un metodo qualitativo, dato che quello quantitativo è basato su analisi statistiche o matematiche e sebbene abbia il pregio di quantificare il rischio attraverso i numeri al contempo le amministrazioni non hanno né personale capace di fare ciò né serie storiche adeguate. Lo sviluppo futuro di *machine learning* e di reti neurali potrebbe rivelarsi utile anche a questo fine, consentendo quindi di propendere per la scelta di questo metodo valutativo.

Un discorso a parte, invece, riguarda la fase di valutazione del rischio in senso stretto, laddove si identificano i comportamenti che potrebbero essere fonte di fatti corruttivi. Infatti, se da un lato l'ausi-

lio dell'algoritmo potrebbe essere utile per affinare la valutazione di esposizione al rischio attraverso gli indicatori di rischio stessi, da un altro lato, però, il contributo degli attori umani rimane determinante nelle restanti fasi del processo. L'ipotesi fino ad ora presa in considerazione concerne le prime due macro-fasi del processo di gestione del rischio ("Analisi del contesto" e "Valutazione del rischio"), dove l'utilizzo delle tecniche di IA è considerato possibile e perfino vantaggioso. Nella terza macro-fase ("Trattamento del rischio"), invece, l'impiego dell'IA non è ritenuto necessario, poiché la funzione svolta nella procedura dagli attori coinvolti risulta essere imprescindibile.

Ad ogni modo, da quanto detto conseguirebbe un cambiamento netto del processo: l'algoritmo sostituirebbe la scelta di molte determinazioni degli interventi organizzativi da adottare nel campo della prevenzione della corruzione.

Sulla base di queste osservazioni si possono brevemente immaginare due possibili scenari: il primo basato su un utilizzo ponderato dell'intelligenza artificiale, ovvero limitatamente ad alcuni campi; l'altro, invece, dove tutte le determinazioni vengono decise dalle procedure automatizzate.

Nel primo caso si tratterebbe quindi di utilizzare il modello di programmazione algoritmica nel seguente modo: di fronte ai rischi x si individuano le misure y , le quali vengono individuate in un'amministrazione attraverso una sequenza logica predeterminata e condizionata dal programmatore.

Quindi, come si può notare, questo tipo di intervento non è definibile come una tecnica di IA pura, in quanto l'elemento umano sarebbe presente e determinante nella fase di programmazione. Questo tipo di utilizzo potrebbe apportare maggiore oggettività e imparzialità della scelta delle misure da adottare, senza eliminare del tutto il contributo dei funzionari.

L'elemento umano continuerebbe a svolgere un ruolo significativo nello sviluppo delle varie fasi della policy anticorruzione. Si verrebbe dunque a prospettare un rapporto tra PA e IA conforme ai principi di sviluppo etico dell'IA²⁶ e coerenti con la logica *govern IA and govern with IA*²⁷. Tale approccio sarebbe d'altronde in linea con quanti nella dottrina italiana, in merito a siffatte questioni, sostengono l'indispensabilità del funzionario umano²⁸.

Diversamente dal primo scenario, qualora si riuscissero ad applicare diffusamente le tecniche di intelligenza artificiale si avrebbero significativi cambiamenti sul vigente processo di gestione del rischio: alcune fasi sarebbero fortemente condizionate dal ricorso alle tecniche IA, alcune verrebbero semplificate e altre eliminate del tutto; il ruolo di alcuni attori verrebbe vanificato dal contributo dell'IA; infine anche la scelta



delle misure concrete da adottare per la prevenzione dei rischi subirebbe una significativa variazione, dato che questa parte della procedura è influenzata dall'analisi svolta in precedenza.

Rimanendo all'ipotesi sopra esposta, infatti, la scelta delle misure dev'essere descritta con accuratezza per porre in rilievo sia l'obiettivo che si intende raggiungere che le modalità adoperate. Stessa cosa è valida per il conseguente processo di programmazione delle misure. Tutto ciò, stando a questa seconda ipotesi, non potrebbe essere garantito e ciò desta non poche perplessità. Questa considerazione, tuttavia, non riguarda solo l'ambito dell'anticorruzione, bensì la possibile applicazione estesa dell'IA, e nello specifico del *machine learning*, nel contesto dell'attività della pubblica amministrazione. In particolare, tali dubbi riguardano le questioni relative sia alla motivazione²⁹ di come si giunge ad un data soluzione sia in merito all'esplicitazione dei fattori che determinato la scelta³⁰ e se si tratta di un sistema basato sull'apprendimento occorre specificare il metodo di addestramento dell'algoritmo utilizzato.

Detto ciò, comunque, non si può escludere che in futuro alcune tecniche IA di questo tipo possano essere adoperate come misure di prevenzione della corruzione. Infatti, le ipotesi sopra avanzate si riferiscono esclusivamente al sistema di definizione dei Ptpct. Meritano invece un discorso a parte quelle misure che grazie all'IA potrebbero, e in alcuni Stati già lo fanno, rappresentare un valido contributo alla causa preventiva della corruzione in senso più ampio.

Oltre alle misure che vengono adottate *nel* sistema di prevenzione (Ptpct) vero e proprio, vi sono inoltre settori in cui l'applicazione di queste tecnologie potrebbe parimenti influire sul sistema di prevenzione. Si tratta di strumenti e settori che, nonostante non siano interni all'impianto preventivo, costituiscono un valido e necessario apporto alla causa dell'integrità della pubblica amministrazione.

I principali ambiti potrebbero essere i seguenti: le procedure di reclutamento del personale della PA; il perfezionamento degli indici *red flags*; l'investimento nel cd. *e-procurement* per prevenire ed individuare la corruzione negli appalti pubblici; l'uso della *blockchain* come strumento per maggiore trasparenza, efficienza e garanzia per l'amministrazione digitale; utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di *whistleblowing*.

2.1. Le procedure di reclutamento del personale della PA

Il reclutamento del personale è considerato dall'A-NAC come una delle principali aree di rischio³¹ e

dunque oggetto di particolare attenzione nell'ottica della prevenzione della corruzione. Infatti, trasparenza e imparzialità sono i requisiti centrali in materia di assunzione del personale all'interno della legge anticorruzione del 2012³².

È da ormai un anno che si stanno sperimentando nuovi meccanismi per la selezione dei candidati nei concorsi pubblici. Tale aspetto si pone in conformità con l'art. 35 del d.lgs. 30 marzo 2001, n. 165, che nel regolare il reclutamento del personale, al comma 3 prevede che la PA può ricorrere: «all'ausilio di sistemi automatizzati, diretti anche a realizzare forme di preselezione».

L'art. 10 del d.lgs. 28 maggio 2021, n. 76³³ ha aperto alle tecniche di IA nell'ambito delle procedure concorsuali per garantire maggiore velocità, efficienza e soprattutto maggior aderenza ai principi costituzionali che regolano l'accesso ai pubblici uffici³⁴.

Le riflessioni debbono essere fatte in termini di costi/benefici: da un lato, la velocizzazione della tempistica di selezione, della correzione delle prove e la possibilità immediata per il candidato di verificare i risultati; dall'altro, emergono alcuni rischi legati al rispetto di una serie di principi delicati.

Le maggiori ricadute positive riguardano sia la procedura che la stessa scelta dei candidati. Lo svolgimento delle prove beneficerebbe di una significativa semplificazione, ma anche una più rapida attribuzione dei risultati ai candidati e quindi si giungerebbe più rapidamente alla formazione delle graduatorie. Da questo punto di vista, dunque, si otterrebbero effetti positivi relativamente sia al buon andamento che all'imparzialità. In quanto, quest'ultimo principio sarebbe garantito dal fatto che nel momento di correzione delle prove verrebbero eliminati sia gli eventuali errori che l'indebita interferenza umana. Si potrebbe dunque ottenere maggiore imparzialità nella scelta dei candidati, per questo motivo ciò potrebbe rappresentare il maggiore vantaggio per la procedura di selezione nella prospettiva della prevenzione dei fatti corruttivi.

La giurisprudenza costituzionale ha designato un vero e proprio rapporto strumentale tra la regola del concorso pubblico e il principio di buon andamento³⁵, ciò si traduce nell'esigenza che le amministrazioni possano dotarsi di personale idoneo per svolgere le funzioni ad essi affidate. L'automatizzazione delle varie fasi concorsuali, attraverso per esempio l'utilizzo di software a lettura ottica OCR consistenti in riconoscimento ottico dei caratteri, comporta un risparmio di tempo, di impiego di risorse di vario tipo e quindi renderebbe l'iter più efficiente ed efficace per quanto riguarda la formazione delle graduatorie nel più breve tempo possibile.



Un altro aspetto positivo è quello che ogni candidato e candidata potrebbero tempestivamente verificare il proprio punteggio e le risposte non corrette, così da poter accedere agli atti (l. 7 agosto 1990, n. 241) senza l'intervento della PA.

I rischi invece sono legati al rispetto di principi molto importanti: alcuni di essi sono interni al già citato comma 3 dell'art. 35 del d.lgs. 165/2001 e altri contenuti nel GDPR³⁶. Nel primo caso, le maggiori preoccupazioni riguardano il principio di pari opportunità tra lavoratrici e lavoratori sancito alla lettera c) del comma 3 dell'art. 35 del d.lgs. 165/2001. Infatti, in tal senso si sono verificati problemi simili nell'esperienza statunitense³⁷: gli algoritmi non avrebbero considerato la parità di genere nel processo di elaborazione degli output. Anche se le discriminazioni potrebbero essere anche di altri tipi³⁸. I problemi legati al GDPR sono rappresentati innanzitutto dall'art. 22 (*Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*)³⁹, dal quale deriva che nei concorsi pubblici bisognerebbe garantire ai candidati una valutazione che non sia totalmente effettuata dai meccanismi automatizzati. Ulteriori preoccupazioni sono dovute alla poca trasparenza del processo di elaborazione del risultato, al trattamento dei dati personali⁴⁰ ed al principio di controllo atto a garantire che gli individui siano attori informati e in controllo delle loro scelte⁴¹.

La recente esperienza applicativa dell'IA ai concorsi pubblici evidenzia vantaggi e pericoli, che potrebbero essere però superati attraverso l'utilizzo di metodi che proteggano i dati e i principi succitati, soprattutto attraverso una chiara regolamentazione.

2.2. Perfezionamento degli indici *red flags*

Sempre nell'ottica di miglioramento dell'analisi del rischio corruttivo, l'ANAC ha promosso, anche attraverso le tecniche IA, alcune ricerche ed iniziative mirate a sviluppare indicatori di rischio più efficaci e distinti per settori e tipologie di amministrazioni⁴². Gli indici *red flags* o indicatori di rischio sono misure sintetiche composte da una o più variabili, che identificano l'esistenza del rischio di corruzione all'interno di specifici processi decisionali⁴³.

Ad oggi, alcuni studi⁴⁴ hanno ipotizzato l'utilizzo di *machine learning* per lo sviluppo di indici capaci di prevedere la corruzione, in particolare nel settore degli appalti pubblici. Sostanzialmente ci si basa su enormi banche dati che raccolgono i vari dati (per es. gli acquisti pubblici) e poi attraverso le tecniche di intelligenza artificiale producono gli indici di rischio. Gli algoritmi identificano e segnalano in modo indipendente quei modelli sospetti che emergono

dai dati e li segnalano a coloro che si occupano dei controlli interni ed esterni all'amministrazione. Il problema derivante da ciò, come in tutti gli altri casi in cui si utilizzano grandi banche dati⁴⁵, è quello della tutelabilità e titolarità del bene posto dalla natura immateriale delle banche dati. Più in generale, verrebbero a configurarsi quegli aspetti problematici legati alla finalità del trattamento dei dati⁴⁶, la lesione del diritto all'autodeterminazione informativa e quindi il rispetto delle disposizioni della normativa privacy sancita dal Regolamento UE n. 2016/679 (GDPR)⁴⁷.

Gli scenari, anche in questo caso, sono diversi in virtù del rapporto tra le tecniche IA e gli attori umani⁴⁸: in un primo scenario, le tecnologie adoperate raccolgono le informazioni, che necessitano della presenza degli analisti umani per rilevare le pratiche corrotte evincibili dai dati; un secondo scenario è quello che consente agli algoritmi di identificare in modo indipendente i modelli sospetti nei dati e segnalarli successivamente agli attori imputati al controllo. Un terzo e per ora più remoto scenario è quello che attribuisce maggiore autonomia agli algoritmi, i quali non solo potrebbero effettuare il processo di rilevazione in modo indipendente, ma anche pubblicare automaticamente i casi sospetti. Senza la presenza degli attori di controllo, tuttavia, le informazioni raccolte dalle tecniche IA potrebbero non tenere conto del fatto che alcune di esse riguardino dati personali che si riferiscono a una persona identificata o identificabile⁴⁹. Un tale scenario si pone inoltre in contrasto con l'art. 22 del GDPR che vieta, come detto, la possibilità che la decisione venga unicamente assunta dai sistemi automatizzati.

In questa ipotesi, pertanto, potrebbero configurarsi rischi concreti per la privacy a causa dell'applicazione totale dell'IA, dove gli attori umani avrebbero unicamente un ruolo marginale, ovvero successivo al processo di rilevazione.

Gli indici *red flags*, quindi, potrebbero essere perfezionati attraverso set di dati, elaborati dagli strumenti IA, utili alla individuazione dei problemi⁵⁰. Il potenziamento di questi indici potrebbe non solo costituire un valido e robusto ausilio alle amministrazioni nel loro processo di monitoraggio e prevenzione del rischio, ma potrebbe anche sviluppare un sistema che sia maggiormente in raccordo con il processo di misurazione e valutazione della performance⁵¹.

2.3. Investimento nel cd. *e-procurement* per prevenire ed individuare la corruzione negli appalti pubblici

I recenti scandali legati agli appalti nel periodo della pandemia hanno riaccessato l'attenzione sulla necessità



di potenziamento del sistema di regolamentazione e controllo di questo settore.

Il Pnrr ha incluso tra i principali obiettivi quello di far evolvere il sistema di *e-procurement* attraverso la digitalizzazione *end-to-end* dei processi di approvvigionamento pubblico⁵² ed in particolare di utilizzare: «intelligenza artificiale/machine learning per l'osservazione e l'analisi delle tendenze nell'uso degli strumenti di acquisto, delle dinamiche di mercato e di spesa e dei comportamenti di pubblica amministrazione e operatori economici⁵³».

Esistono già studi e primi approcci⁵⁴ (su uno di essi si dirà meglio nel paragrafo successivo) circa il possibile contributo che le tecniche IA potrebbero dare alla causa dell'anticorruzione nella sfera degli appalti pubblici. L'affinamento degli indici *red flags*⁵⁵ è in realtà solo una delle componenti che potrebbe costituire un vero e proprio irrobustimento del, già esistente, sistema di *e-procurement*.

Nella prospettiva anticorruzione, l'ausilio di meccanismi IA potrebbe comportare vantaggi di tipo incrementale, senza però alterare in modo significativo (o sostituire) le architetture di supervisione e applicazione esistenti⁵⁶. L'IA insomma potrebbe aiutare in termini di controllo e di individuazione della potenziale corruzione ed esonerare gli attori umani da tale compito.

Anche nel settore del *public procurement*, quindi, l'IA non apporterebbe modifiche rivoluzionarie rispetto alle attuali modalità di prevenzione e controllo previste dalla disciplina italiana. Il maggiore vantaggio consisterebbe nell'offrire un notevole incremento e accelerazione dei controlli anticorruzione, con il beneficio di poter effettuare in anticipo i relativi interventi.

L'utilizzo del *machine learning* e le tecniche di *text-mining*⁵⁷ si basano su cospicue fonti di dati, tipo quelli contenuti nelle documentazioni di gara, per poter individuare segnali di corruzione nel processo degli appalti⁵⁸.

La tecnologica *blockchain* potrebbe essere un ulteriore valore aggiunto per il rafforzamento dell'*e-procurement*, soprattutto in merito ad un potenziamento della digitalizzazione delle procedure di affidamento degli appalti già in vigore e degli acquisti. In tal modo, si avrebbe senz'altro un miglioramento dei principi di imparzialità e buon andamento, ma consentirebbe anche di far sì che questi metodi siano quelli prevalenti nell'attività delle stazioni appaltanti. Per giunta, i registri distribuiti potrebbero risultare utili per la gestione dei dati degli operatori economici e per accelerare l'attività istruttoria della stazione appaltante. La finalità di questo tipo di intervento è quello di scongiurare la presenza di false dichiarazioni all'interno dei documenti di gara e inoltre per limitare

la relativa valutazione discrezionale da parte della stazione appaltante.

2.3.1. L'uso della blockchain come strumento per maggiore trasparenza, efficienza e garanzia per l'amministrazione digitale

Rispetto ai registri *blockchain*, si è già detto che potrebbero fungere da maggiore promessa di trasparenza generale per la PA, ma si riportano tuttavia i benefici specifici derivanti da essi: tracciamento sicuro e trasparente delle informazioni e dei dati; immodificabilità e tracciabilità nella gestione dei dati; utilizzabilità e validità in diversi ambiti; maggiore automatizzazione dei processi; rafforzamento della fiducia tra cittadini e le pubbliche amministrazioni; migliore e più efficiente gestione documentale; maggiore interoperabilità tra le varie PA; maggiore trasparenza dei processi interni.

Da queste conseguenze positive ne deriva che il sistema di prevenzione della corruzione potrebbe essere uno dei settori più idonei a sfruttare le potenzialità messe a disposizione da questi registri. Le tecnologie *blockchain* stanno attirando le comunità anticorruzione per il loro potenziale di prevenzione della corruzione e per la garanzia di protezione dei registri pubblici da frodi e manomissioni⁵⁹. La *blockchain* scongiura la probabile manomissione dei registri, in quanto non consentirebbe ai dipendenti di apportare modifiche e falsificare le voci interne ad essi.

È dunque auspicabile che la pubblica amministrazione italiana e l'ambito di prevenzione possano usufruire diffusamente di questo sistema, soprattutto nella prospettiva dell'auspicata trasparenza algoritmica⁶⁰.

2.4. Utilizzo esclusivo di strumenti di crittografia per le segnalazioni in materia di *whistleblowing*

In tema di segnalazioni anonime di illeciti, l'ordinamento italiano è tuttora in corso di adeguamento alla direttiva (UE) 2019/1937 in materia di *whistleblowing*. A parte ciò, è auspicabile anche in questo campo l'adozione dell'IA per le procedure di acquisizione e gestione delle segnalazioni anonime.

L'attuale disciplina italiana si sviluppa in concreto con la presentazione delle segnalazioni mediante diversi canali, anche se l'utilizzo della piattaforma è ritenuto prioritario.

La procedura si basa su un protocollo di crittografia, che è un sistema basato sull'uso di un algoritmo matematico che agisce su una serie di caratteri. Tale sistema garantisce il trasferimento di dati riservati e, in seguito alla segnalazione, genera un codice identificativo univoco registrato sul portale ANAC, che permette



al *whistleblower* di comunicare in modo anonimo con l'autorità. I dati che vengono comunicati sono poi segregati all'interno di un'apposita sezione della piattaforma, la quale è inaccessibile anche all'ufficio per la vigilanza sulle segnalazioni dei *whistleblowers* (UWHIB). Questa procedura assicura maggiore riservatezza e celerità delle procedure, anche se ad oggi, nonostante questa tipologia sia quella raccomandata dall'ANAC, non è imposta nell'attuale l. 30 novembre 2017, n. 179⁶¹. Anche nelle linee guida ANAC del 2021, quando si parla di modalità di gestione delle segnalazioni, si afferma che: «le Amministrazioni sono, quindi, tenute a disciplinare, in conformità alle presenti Linee guida, le procedure, preferibilmente informatizzate, per la ricezione e gestione delle segnalazioni».

Appare essenziale investire solo su questo tipo di tecnologie ai fini di una maggiore conformazione ai principi sanciti all'art. 9 della direttiva del 2019 e per superare alcuni problemi recentemente sollevati dal Garante della privacy⁶².

Le tecniche IA potrebbero servire per perfezionare l'operazione di crittografia attualmente adoperata. Per esempio, ci sono modelli proposti che basano le procedure di segnalazione sul sistema *blockchain*, che si avvale di una crittografia asimmetrica. In particolare, le proprietà dei registri distribuiti e l'affidabilità delle cd. *ring signatures* creerebbero maggiori condizioni favorevoli non solo per la procedura stessa, ma potrebbero infondere maggiore fiducia e incentivi al *whistleblower*⁶³ nell'effettuare la segnalazione.

3. Alcune esperienze concrete di applicazione IA nel campo anticorruzione a livello globale

Il recente sviluppo di iniziative basate su strumenti IA, finalizzate a perfezionare le strategie anticorruzione, ha creato un alto livello di aspettative⁶⁴, ma ha consentito inoltre una prima comprensione su vantaggi e difficoltà derivanti da queste nuove pratiche⁶⁵.

Si descrivono sinteticamente le seguenti esperienze: il sistema di allerta precoce dei ricercatori dell'Università di Valladolid; l'operazione *Serenada de amor* in Brasile; *ProZorro* in Ucraina nel campo dell'*e-procurement*.

Il sistema di allerta precoce dei ricercatori dell'Università di Valladolid

Due ricercatori dell'Università di Valladolid hanno sviluppato un modello basato su reti neurali, attraverso mappe auto-organizzate, per prevedere in quali province spagnole⁶⁶ potrebbero verificarsi casi di corruzione⁶⁷, sulla base di vicende che sono state affrontate dai media o che sono già andate a processo.

Il sistema fornisce alcuni dati che indicano un'alta probabilità di corruzione, anche se gli stessi autori tengono a sottolineare che ciò non significa che la corruzione accada effettivamente. Dallo studio emerge che ci sono una serie di fattori economici e politici che consentono di creare un attendibile sistema di allerta precoce. I principali fattori che favorirebbero la corruzione sono: la tassazione e l'aumento dei prezzi degli immobili, la crescita economica, il numero crescente di istituti di deposito e società non finanziarie; la presenza di uno stesso partito politico al potere per lunghi periodi. Occorre però riportare alcune precisazioni sui fattori appena indicati. La crescita economica o il fatto che un determinato partito rimane al potere a lungo non sono direttamente cause di corruzione pubblica. La ricerca considera invece che le zone a più rapida crescita o quelle governate dallo stesso partito per lungo tempo potrebbero essere più soggette a casi di corruzione. La crescita economica, quindi, non è un pericolo o un fattore corruttivo di per sé, ma laddove si verifica aumentano le interazioni tra gli agenti economici e i funzionari pubblici e questo potrebbe determinare anche l'insorgere di alcune relazioni opache. Stessa cosa è valida per i partiti che rimangono a lungo tempo al potere: tale situazione potrebbe favorire la presenza di rapporti clientelari e sleali tra i politici e gli operatori economici. Mentre la presenza di mercati più competitivi può comportare la diffusione di influenze di agenti che vogliono ottenere a tutti i costi, ad esempio attraverso tangenti o la promessa di compensi di ogni tipo, concessioni o affidamenti di varia natura.

Tale sistema fornisce diversi profili di rischio di corruzione a seconda delle condizioni economiche di una regione e della tempistica della previsione: consente infatti di prevedere la corruzione fino a tre anni prima che i casi vengano rilevati, in altri casi fornisce previsioni più nel breve termine e in questi casi gli studiosi suggeriscono l'adozione di misure preventive più urgenti.

Lo studio si è basato su tutti i casi di corruzione comparsi in Spagna tra il 2000 e il 2012, tra cui casi celebri come il caso Mercasevilla e il caso Baltar. Il metodo di raccolta e di analisi delle informazioni è stato eseguito con le reti neurali, che hanno consentito di rilevare i fattori più predittivi di corruzione.

Il principale punto di forza e di innovatività di questo metodo sta proprio nel fatto che si è basato su un database di dati reali, a differenza della stragrande maggioranza degli indici che si basano prevalentemente sulla percezione della corruzione⁶⁸.

L'esperimento proposto dagli studiosi spagnoli può offrire una serie di vantaggi: rafforzamento della logica preventiva, in quanto il sistema di allerta precoce ha esclusivamente questa finalità; potrebbe costituire



un correttivo molto importante per la policy anticorruzione di tutti i paesi al fine di rendere più efficaci le misure e per utilizzare un sistema più sostenibile anche dal punto di vista delle risorse impiegate; considerare la programmazione *machine learning*, *deep learning* nello specifico, come un tipo di IA che se usato nel giusto modo può costituire un serio alleato per la causa dell'anticorruzione.

Operazione Serenada de amor in Brasile

L'operazione *Serenada de amor*, esempio di strategia anticorruzione dal basso⁶⁹, consiste in un progetto di intelligenza artificiale finalizzato all'analisi della spesa pubblica in Brasile. L'iniziativa è partita nel 2016 dal *data scientist* Irio Musskopf, il quale è stato in grado di fornire le risorse necessarie per sviluppare il sito web che attualmente conta un nutrito gruppo di persone e più di 600 componenti del gruppo Telegram. La realizzazione del progetto è stata possibile attraverso una campagna di auto finanziamento e attraverso la collaborazione con il sito GitHub che è un servizio di hosting per progetti software. Il sito web su cui si basa l'iniziativa è il risultato di un progetto tecnologico che ha cercato di utilizzare l'intelligenza artificiale, *machine learning* in particolare, per controllare i conti pubblici dei politici brasiliani, con l'obiettivo di favorire un vero e proprio monitoraggio diffuso. Il sito *Serenada de amor*⁷⁰ è stato sviluppato con dati pubblici aperti, consentendo pertanto a qualsiasi cittadino di esaminare l'impiego della quota dedicata all'esercizio delle attività parlamentari (CEAP) dei deputati federali e dei senatori brasiliani relativamente al rimborso di varie spese, come il vitto, trasporto, alloggio e attività educative e culturali.

La pagina web ha sviluppato un robot open source chiamato *Rosie*, che analizza le spese rimborsate ai deputati e senatori, individuando sospetti e favorendo il controllo sociale della spesa pubblica. Le tecniche usate si basano sull'apprendimento automatico che consente di individuare i rimborsi anomali nel CEAP, i cui risultati vengono successivamente pubblicati sui social media in modo che i cittadini possano visualizzarli, indagare, interrogarli e persino segnalarli. Al fine di consentire ai cittadini la comprensione delle informazioni generate da *Rosie*, il sito ha creato un apposito software *Jarbas*, che facilita la verifica delle informazioni relative al rimborso delle spese dei parlamentari.

Sono passati un po' di anni dallo sviluppo di questa esperienza e, nonostante l'impatto innovativo e la natura *bottom-up* del progetto, emergono alcuni elementi che portano alla luce la difficoltà di utilizzo diffuso di questo sistema. Le caratteristiche che quest'approccio porta con sé evidenziano che, nonostante l'ausilio dell'IA, rimane centrale il ruolo delle persone

nel verificare i sospetti rilevati dai bot. Proprio per questo motivo, la partecipazione delle persone è minacciata e disincentivata, in questo tipo di iniziative, da alcune conseguenze problematiche che potrebbero tradursi in forme ritorsive vere e proprie o potrebbero comportare citazioni in giudizio.

ProZorro in Ucraina

La piattaforma di *e-procurement ProZorro*, basata sull'utilizzo di IA e di *machine learning*, è stata sviluppata da attivisti e volontari ed è entrata in vigore nel 2015, quando in Ucraina si avvertiva una forte necessità di varare una serie di riforme anticorruzione⁷¹. Il sistema che sta alla base di *ProZorro* è caratterizzato dal fatto che permette di condurre gare d'appalto in condizioni di totale apertura in tutte le fasi dell'acquisto e offre le stesse condizioni di partecipazione agli appalti pubblici. La finalità del progetto è infatti quella di sollecitare il coinvolgimento di nuovi fornitori che non hanno mai partecipato alle gare pubbliche e quindi aumentare la concorrenza nel settore. Per giunta, si consente un controllo vero e proprio sull'utilizzo dei fondi in modo trasparente ed efficiente.

Gli specialisti di *ProZorro* hanno introdotto un sistema elettronico di appalti pubblici basato su un modello multipiattaforma, che ha consentito loro di utilizzare i servizi di tante piattaforme elettroniche commerciali già attive in Ucraina: il portale *prozorro.gov.ua* scambia in modo automatico le informazioni e i documenti con le altre piattaforme elettroniche. Nella piattaforma principale sono riportate le caratteristiche degli appalti pubblici ripartiti per dimensione, in particolare: sottosoglia, sopra soglia, soglie speciali e le procedure per tre tipi principali di appalto pubblico (gara d'appalto aperta, gara d'appalto a partecipazione limitata, dialogo competitivo) e una aggiuntiva (appalto a procedura negoziata).

Gli appalti pubblici attraverso *ProZorro* agiscono come una sorta di meccanismo di controllo statale sulla regolazione delle condizioni di mercato, rappresentando di conseguenza un valido strumento per prevenire la corruzione in questo settore.

Le prime analisi mostravano l'esistenza di una tendenza negativa della concorrenza e la riduzione dell'ammontare dei risparmi nei fondi pubblici. *ProZorro* ha diffuso inoltre tutte le informazioni sugli appalti governativi, oltre a creare tanti dati standardizzati utili sia per il controllo che per l'analisi.

Da alcune stime risulta che il sistema abbia ridotto in modo notevole la corruzione: attraverso aste online trasparenti e controllo pubblico, ha consentito allo Stato di risparmiare parecchi fondi pubblici⁷².

ProZorro dimostra insomma che big data e open data possono essere considerati come mezzi seri per



monitorare e prevenire la corruzione. Ovviamente, come per ogni potenziale strumento IA nel campo dell'anticorruzione, anche questo sistema dev'essere integrato in un sistema di controllo più ampio, collegato con la legislazione in materia e con un ruolo determinate dell'autorità/agenzia anticorruzione.

4. Quali sfide e rischi ne derivano in termini di legalità e partecipazione?

Nelle pagine precedenti si è cercato di considerare come e in quali casi l'intelligenza artificiale potrebbe essere utile per perfezionare e semplificare (misure e risorse) il sistema della prevenzione della corruzione. Tralasciando le esperienze brevemente descritte, si vuole circoscrivere il raggio della riflessione alla pubblica amministrazione, al fine di considerare il probabile impatto dell'IA sulla legalità⁷³ e la partecipazione per quanto riguarda lo sviluppo dei Ptpct.

Relativamente alla cd. "legalità algoritmica" e alla crisi di legittimità dello Stato amministrativo automatizzato⁷⁴ si è già discusso ampiamente, soprattutto in relazione al tema della decisione amministrativa e della discrezionalità, alle prime valutazioni e sentenze del giudice amministrativo in materia⁷⁵; alla compatibilità dell'algoritmo, a date condizioni⁷⁶, con l'attività e l'organizzazione della pubblica amministrazione.

Nel caso in cui il processo che porta all'adozione dei piani di prevenzione fosse interamente governato dall'IA, l'attuale iter di predisposizione dovrebbe essere completamente rielaborato in virtù del venir meno di importanti elementi costitutivi. Nelle fasi del processo di gestione del rischio, come già affermato, è determinante il ruolo del funzionario umano, soprattutto per motivi insiti nella legalità amministrativa. Come noto, il piano è un documento di natura programmatoria determinato da caratteristiche, garanzie e responsabilità simili ad un procedimento amministrativo⁷⁷: motivazione delle scelte adottate; ruolo di coordinamento del processo di gestione del rischio affidato a un responsabile (Rpct); l'ascolto e la partecipazione degli *stakeholder*.

Nonostante la l. 6 novembre 2012, n. 190 non sancisca espressamente l'obbligo della motivazione delle misure organizzative assunte, ciò è deducibile indirettamente all'interno dei piani nazionali anticorruzione dell'ANAC e direttamente nell'allegato 1 del PNA del 2019⁷⁸.

Ogni decisione che viene presa in merito alle singole fasi del Ptpct dev'essere motivata al fine di garantire la massima trasparenza, nonché per rendere ragione del perché sono state preferite alcune soluzioni rispetto ad altre e con quali vantaggi. In particolare, le scelte che necessitano della motivazione

sono le seguenti: approccio valutativo, rilevazione dei dati e delle informazioni, misurazione applicata e le modalità di campionamento utilizzate.

Nell'analisi del rischio un fattore determinante è la scelta dell'approccio valutativo. I criteri di valutazione che vengono scelti debbono essere valutati e motivati per ridurre l'autoreferenzialità della scelta e per fornire le conseguenti evidenze a supporto. Dato che si tratta di un documento di programmazione, un'altra motivazione che dev'essere resa è quella legata alla scelta del tipo di campionamento usato per il monitoraggio del piano, che può essere di tipo statistico o ragionato. Un'ultima motivazione è quella della cd. "misurazione applicata" relativa alla rilevazione e alla valutazione del livello di esposizione al rischio, consistente in una valutazione complessiva basata sui singoli indicatori.

La completa assunzione dei compiti da parte della macchina eliminerebbe inoltre il ruolo di coordinatore del processo di predisposizione del piano affidato al responsabile (Rpct). Tale aspetto contribuirebbe a due conseguenze negative: mancanza di un soggetto sul quale far ricadere eventuali responsabilità legate alla procedura; contrasto con i poteri e le funzioni attribuite al Rpct dalla legislazione vigente. Si delinea quindi una vera e propria incompatibilità tra la totale decisione automatizzata e il Rpct, almeno all'interno del processo di gestione del rischio.

Un'altra questione molto importante è quella legata alle probabili discriminazioni scaturite dalle misure di prevenzione, qualora venissero decise completamente dall'algoritmo. Potrebbero essere adottate misure caratterizzate da una profilazione di criteri stereotipati e discriminatori. Ciò potrebbe accadere a causa di problemi di apprendimento, ovvero: «dalla gestione non corretta dei dati presi in considerazione nella fase in cui il software elabora i propri modelli decisori»⁷⁹. L'approccio di genere nei piani è molto importante per valutare le variabili biologiche, ambientali e sociali, al fine di migliorare l'appropriatezza degli interventi di prevenzione e far sì che la dimensione di genere contribuisca a evitare stereotipi e a definire strategie volte ad evitare disuguaglianze⁸⁰. Questo pericolo potrebbe essere evitato attraverso la preliminare programmazione se si trattasse dell'IA *rule-based programming*; invece, si riscontrerebbero serie difficoltà di fronte alla tipologia *machine learning*.

Alla luce di ciò, si pone dunque un serio problema di disparità di trattamento dei destinatari delle misure decise dall'IA, in chiaro contrasto con gli artt. 3 e 97 Cost. e nel caso di discriminazione di genere anche degli artt. 7 e 35 del d.lgs. n. 165/2001.

Un ultimo elemento è quello della protezione dei dati ai sensi del Regolamento (UE) 2016/679. Infatti,



uno dei primi step dell'iter di approvazione dei Ptpct consiste in un'ampia raccolta di dati (fonti interne ed esterne), che possono poi confluire in banche dati digitali. Alcuni di questi dati, tuttavia, sono soggettivi e ricavati dagli *stakeholder* relativi alla percezione che questi hanno del fenomeno corruttivo e che per questo motivo rappresentano dati personali.

Anche in questo caso, bisogna formulare due distinte ipotesi: 1) utilizzo limitato dell'IA *rule-based programming*, dove il programmatore umano inserisce i dati nel rispetto della normativa GDPR; 2) se, invece, l'elemento umano fosse esterno, l'algoritmo non sarebbe quasi certamente capace di rispettare questi principi.

L'applicazione estesa dell'IA al sistema appena illustrato comporterebbe: a) l'impossibilità di esprimere le motivazioni delle scelte determinate dalle procedure automatizzate; b) scarsa, se non assente, *explainability* del processo decisionale, ovvero come si arriva dall'input all'output⁸¹; c) il difficile rapporto tra il processo di elaborazione automatizzata delle misure di prevenzione e il rischio che le misure possano essere discriminatorie nei confronti dei funzionari e delle funzionarie; d) le questioni problematiche legate alla protezione della privacy e dei dati adoperati nel processo di gestione del rischio.

Se si trattasse di ricorrere alle tecniche IA limitatamente ad alcuni elementi, ciò permetterebbe di mantenere salvo l'attuale impianto dell'approvazione dei Ptpct e, come detto, favorirebbe un significativo efficientamento sia della gestione dei dati grazie alle tecniche *blockchain* che della bontà degli indicatori di rischio adoperati attraverso la definizione di tecniche IA e di *machine learning*.

Viceversa, se il ruolo cruciale e onnipresente del funzionario (specie del Rpct) venisse soppiantato da forme di IA capaci di fare a meno del contributo umano, due sarebbero le possibili conseguenze: 1) si dovrebbe accantonare il sistema finora adottato e varare un'adeguata regolamentazione, nella quale l'intervento umano sarebbe esterno al processo ma che potrebbe garantire il controllo *ex-post* sulle misure; 2) tale ipotesi non dovrebbe essere ritenuta praticabile in quanto verrebbero meno delle garanzie legali molto importanti.

4.1. Segue. Prevenzione della corruzione e partecipazione

Nel framework italiano di prevenzione della corruzione la partecipazione assume un ruolo molto importante ed è estesa a tanti soggetti e fasi, sia interni che esterni alla pubblica amministrazione.

La logica preventiva infatti confida nel personale dell'amministrazione sia per la promozione e il rispetto di doveri e misure che per il contributo in fase di formazione e aggiornamento dei Ptpct e dei codici di comportamento. I piani di prevenzione vedono un diretto coinvolgimento di vari soggetti interni alla struttura e degli *stakeholder* sia interni che esterni. Infatti, oltre al Responsabile sono coinvolti nel processo di gestione del rischio tanti altri uffici, organismi, la dirigenza e il personale dipendente. Oltre all'organigramma vero e proprio, vi sono gli *stakeholder* ovvero quegli altri uffici che vengono informati e invitati ad esprimere pareri sulla bozza di piano che poi verrà adottata. È previsto anche un contributo partecipativo dei cittadini e delle organizzazioni portatrici di interessi, che possono essere consultati e a loro volta possono far pervenire le proprie osservazioni e suggerimenti nella fase di aggiornamento⁸². Ciò si concretizza con l'invio delle proposte attraverso un apposito modulo allegato all'indirizzo e-mail del responsabile, tramite pec o in una sezione dedicata del portale web dell'amministrazione⁸³.

Premesso ciò, anche l'elemento partecipativo verrebbe dunque notevolmente compromesso nel caso in cui gli algoritmi venissero utilizzati in modo estensivo nel processo di adozione dei Ptpct. Se la scelta delle misure fosse completamente scaturita dalle procedure automatizzate, il contributo dei soggetti interni ed esterni non avrebbe senso e quindi verrebbe meno un pilastro dell'attuale sistema *bottom-up* di co-definizione delle misure, nel quale anche i soggetti esterni all'amministrazione vengono coinvolti in una logica di cittadinanza amministrativa partecipe e attenta alla buona amministrazione⁸⁴.

L'ipotetico sistema di definizione delle misure basato esclusivamente sull'IA si pone inoltre come paradossale rispetto alla maggioranza dei casi in cui, l'utilizzo estensivo delle ICT, rideterminerebbe in positivo il ruolo tra cittadino e amministrazione sul profilo della partecipazione ai processi decisionali⁸⁵. Un simile impianto, tra l'altro, si porrebbe in chiaro contrasto con le raccomandazioni internazionali in tema di anticorruzione e integrità pubblica (Ocse su tutti⁸⁶), dove alla partecipazione viene conferito un valore di primaria importanza.

Le ripercussioni escludenti in tema di partecipazione sarebbero estese anche alla fase di adozione e revisione dei codici di comportamento delle singole amministrazioni: i doveri integrativi delle PA devono essere adottati sulla base delle evidenze e misure risultanti dal processo di *risk assessment* dei Ptpct; inoltre l'art. 54, co. 5 del d.lgs. n. 165/2001 prevede una "procedura aperta alla partecipazione" per l'adozione e la revisione dei codici di amministrazione. Di conse-



guenza, le regole di condotta dei codici, che appunto sono collegate con i piani, sarebbero prive del momento partecipativo iniziale dei soggetti interni ed esterni all'amministrazione, le cui procedure di presentazione delle istanze sono simili a quelle dei Ptpct.

Il contesto appena ipotizzato, nel quale l'IA escluderebbe la partecipazione interna ed esterna, si pone inoltre in controtendenza con le esperienze di controllo e prevenzione della corruzione dal basso, come i casi sopra descritti⁸⁷. In effetti, in un clima di crescente coinvolgimento dei cittadini alla causa preventiva, in alcuni casi in forma autonoma e in altri attraverso collaborazioni sinergiche con le istituzioni, si andrebbe a compiere un significativo passo indietro. Il sistema di prevenzione della corruzione italiano, indicato da tanti come un *framework* ideale anche per il fattore partecipativo e l'attuazione della politica dal basso, rinunciarebbe quindi ad un suo fattore costitutivo. Di conseguenza, di fronte ad uno scenario così configurato, sorge il dubbio se abbia ancora senso continuare a parlare del modello anticorruzione attuale o se invece, in base alle condizioni ipotizzate, sia piuttosto il caso di parlare di abrogazione della legge 190/2012 e di sollecitare il Parlamento italiano a legiferare in merito ad un nuovo impianto dove il processo di definizione delle misure sarà governato dagli algoritmi e non più dall'essere umano.

5. Riflessioni conclusive

Sebbene nelle pagine precedenti si possa scorgere un certo pessimismo circa la fattibilità di impiego dell'IA nel processo di adozione dei Ptpct e nell'organizzazione preventiva *tout-court*, in realtà si tratta solo di ragionare su alcune questioni controverse ed eventuali cautele da dover adottare⁸⁸.

L'indubbio apporto in termini di efficientamento, risparmio di risorse e di perfezionamento di alcuni strumenti induce senz'altro a sperare che tali tecniche vengano utilizzate nel campo dell'anticorruzione. Tuttavia, però, bisogna riconoscere che l'intervento umano nel processo di gestione del rischio e in altri campi non può essere eliminato o marginalizzato a mero controllo successivo all'adozione delle misure. L'attuale impianto infatti è stato concepito dal legislatore del 2012 come un vero e proprio investimento sul personale e sulla capacità delle amministrazioni di implementare la policy in modo proattivo e partecipato. Si tratta dunque di effettuare un bilanciamento tra i rischi e i benefici che si ripercuoterebbero sulla legalità, l'imparzialità e buon andamento. Detto in altre parole, non possiamo solo considerare gli eventuali vantaggi per quanto concerne una maggiore efficienza ed economicità del processo, bensì bisogna avere la

consapevolezza di cosa potremmo perdere anche in termini di deficit legale.

La proposta che emerge da questo contributo è quella di auspicare un sistema che si possa avvalere dell'IA e non che, viceversa, il contributo umano venga rimpiazzato dagli algoritmi. Appare alquanto sostenibile uno scenario in cui il funzionario umano, preservando una certa "meta-autonomia"⁸⁹, possa continuare a svolgere un ruolo determinante nel campo dei piani anticorruzione, ma utilizzando strumenti e tecniche IA in grado di facilitare i vari processi, perfezionare la gestione dei dati e fornire indici e segnali di allarme più precisi ed attendibili per le successive scelte da prendere.

Stesse considerazioni sono valide per quegli ambiti che non fanno parte del sistema della prevenzione della corruzione, ma che assurgono a presidio dell'integrità della PA. In questi casi, risulterà necessario prevedere meccanismi e garanzie che possano scongiurare eventuali discriminazioni prodotte dalle procedure automatizzate e a far sì che il trattamento dei tanti dati operati dall'IA avvenga nel rispetto della normativa di privacy e protezione dei dati personali.

In conclusione, al di là degli scenari prefigurati, sarà fondamentale la regolamentazione dell'IA in tutto il settore pubblico e soltanto dopo le pubbliche amministrazioni potranno essere in grado di sistematizzare l'impiego dell'intelligenza artificiale in ogni ambito e nel sistema della prevenzione della corruzione in particolare.

Le difficoltà, come detto, sono molte ma occorre affrontarle in modo organico senza pregiudizi e senza sottovalutazioni, altrimenti le questioni attuali potrebbero moltiplicarsi anziché diminuire. L'IA è infatti un mezzo creato per risolvere problemi precedentemente irrisolti, non per risolvere problemi che si devono prima creare.

Note

¹A. PETHERAM, W. PASQUARELLI, R. STIRLING, *The Next Generation of Anti-Corruption Tools: Big Data, Open Data & Artificial Intelligence*, in "Oxford Insights", 2019; N. KÖBIS, C. STARKE, I. RAHWAN, *Artificial Intelligence as an Anti-Corruption Tool. Potentials and Pitfalls for Top-down and Bottom-up Approaches*, in "arXiv.org", 2021; M.S.M. LIMMA, D. DELEN, *Predicting and explaining corruption across countries: A machine learning approach*, in "Government information quarterly", vol. 37, 2020, n. 1; N. Kossow, *Digital anti-corruption: hopes and challenges*, in A. Mungiu-Pippidi, P. Heywood (eds.), "A Research Agenda for Studies of Corruption", Edward Elgar Publishing, 2020; P. AARVIK, *Artificial Intelligence - A promising anti-corruption tool in development settings?* U4: Anti-Corruption Resource Center, 2019; F. ODILLA, *Avoiding minority reports: using AI responsibly in anti-corruption*, in "Corruption, Justice and Legitimacy Program", 2022; V. SHARMA, *Can artificial intelligence stop*



corruption in its tracks?, in “World Bank Blog”, 2019; I. ADAM, M. FAZEKAS, *Are emerging technologies helping win the fight against corruption? A review of the state of evidence*, in “Information Economics and Policy”, vol. 57, 2021; I. VILLAMIL, J. KERTÉSZ, J. WACHS, *Computational Approaches to the Study of Corruption*, in “arXiv.org”, 2022; K. SCHEER, T. RABLE, N. KÖBIS, *AI-Based Software as Anti-Corruption Agent and Its Influence on Employees’ Likelihood of Whistleblowing*, in S. Taneja (eds.), “Academy of Management. Proceedings”, vol. 1, Briarcliff Manor, 2022.

²OECD, *Analytics for Integrity. Data driven approaches for enhancing corruption and fraud risk assessments*, 2019.

³Tale termine è rinvenibile in I.M. DELGADO, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in “Istituzioni del Federalismo”, 2019, n. 3, p. 645.

⁴Sul sistema italiano di prevenzione della corruzione si vedano R. CANTONE, *Il sistema della prevenzione della corruzione*, Giappichelli, 2020; F. MERLONI, *Corruption and Public Administration. The Italian Case in a Comparative Perspective*, Routledge, 2018; E. CARLONI, M. GNALDI, *Understanding and Fighting Corruption in Europe. From Repression to Prevention*, Springer, 2021; R. CANTONE, E. CARLONI, *La prevenzione della corruzione e la sua Autorità*, in “Diritto Pubblico”, 2017, n. 3, pp. 903-944.

⁵Si veda in tal senso S. BATTINI, V. LOSTORTO, *Il ruolo della formazione nella politica di prevenzione della corruzione*, in L. Donato (a cura di), “Gli appalti pubblici tra istanze di semplificazione e normativa anticorruzione. Alla ricerca di un equilibrio tra legalità ed efficienza”, serie Quaderni di Ricerca Giuridica, 2020, n. 89, pp. 225-242.

⁶OECD, *Recommendation of the Council on Public Integrity*, 2017.

⁷In generale sull’IA si vedano P. NORVIG, *Artificial Intelligence: A Modern Approach*, Prentice Hall, 2020; C. BARTNECK, C. LÜTGE, *What Is AI?* in C. Bartneck, C. Lütge, A. Wagner, S.W. An (eds.), “Introduction to Ethics in Robotics and AI”, Springer, 2021; K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro della IA*, il Mulino, 2021.

⁸N. HEATH, *What is artificial general intelligence?*, August 22, 2018.

⁹M. MITCHELL, *Artificial Intelligence: A Guide for Thinking Humans*, Farrar Straus & Giroux, 2019.

¹⁰Sulla relazione tra *machine learning* e decisione amministrativa si veda C. COGLIANESE, D. LEHR, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, Faculty Scholarship at Penn Carey Law, 2017.

¹¹Una rete neurale artificiale è in grado di gestire astrazioni sofisticate, utilizzando i suoi strati nascosti per apprendere la presenza di caratteristiche astratte contenute nei dati. Una semplice rete neurale è organizzata in diversi strati di neuroni.

¹²Così C. CASONATO, *Giustizia e intelligenza artificiale: considerazioni introduttive*, in “BioLaw Journal”, 2021, n. 2, pp. 359-365.

¹³Un esempio è il cd. *Rule-based machine learning* (RBML), consistente in un metodo di apprendimento automatico che identifica, apprende o fa evolvere “regole” da archiviare, manipolare o applicare. Sempre sul tema, si vedano R. EL HAMDANI, M. MUSTAPHA, D. RESTREPO AMARILES et al., *A combined rule-based and machine learning approach for automated GDPR compliance checking*, in “ICAIL ’21: Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law”, 2021, pp. 40-49; Ö. UZUNER, X. ZHANG, T. SIBANDA, *Machine Learning and Rule-based Approaches to Assertion Classification*, in “Journal of the American Medical Informatics Association”, vol. 16, 2009, n. 1, pp. 109-115.

¹⁴Sul legame big data-intelligenza artificiale per la lotta alla corruzione si rinvia a EUROPEAN PARLIAMENT, *Workshop on:*

Use of big data and AI in fighting corruption and misuse of public funds - good practice, ways forward and how to integrate new technology into contemporary control framework, 2021.

¹⁵Così J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in “Public Law Research paper in the age of big data”, 2017, p. 6.

¹⁶Cfr. A. LE SUEUR, *Robot Government: Automated Decision-making and its Implications for Parliament*, in A. Horn, A. Le Sueur (eds.), “Parliament: Legislation and Accountability”, Hart Publishing, 2016, p. 18.

¹⁷Tali obiettivi e azioni sono individuati nel recente documento MINISTERO DELL’UNIVERSITÀ E DELLA RICERCA, MINISTERO DELLO SVILUPPO ECONOMICO E MINISTRO PER L’INNOVAZIONE TECNOLOGICA E LA TRANSIZIONE DIGITALE (a cura di), *Programma strategico. Intelligenza artificiale 2022-24*, 2021.

¹⁸*Ivi*, p. 10. Con il decreto interministeriale 6 dicembre 2021 è stato istituito un fondo per interventi volti a favorire lo sviluppo delle tecnologie e delle applicazioni di intelligenza artificiale, *blockchain* e *Internet of Things*.

¹⁹I. KANT, *Metafisica dei costumi*, Laterza, 2009.

²⁰S. KIERKEGAARD, *Aut-aut*, Mondadori, 2016.

²¹Così M. D’ANGELOSANTE, *La consistenza del modello dell’amministrazione ‘invisible’ nell’età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni*, in S. Civitarese Matteucci, L. Torchia (a cura di), “A 150 anni dall’unificazione amministrativa italiana. La tecnificazione”, vol. IV, La tecnificazione, Firenze University Press, 2016, p. 159 ss.

²²Consiglio di Stato sez. VI, 8 aprile 2019, n. 2270.

²³L’applicazione di questa tecnica nella PA dovrebbe incrementare il livello di fiducia, sicurezza e trasparenza, così in THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM, *Blockchain for Government and Public Services*, 2018.

²⁴Secondo l’ANAC le principali fonti sono queste: riguardo alle fonti esterne, l’amministrazione può reperire una molteplicità di dati relativi al contesto culturale, sociale ed economico attraverso la consultazione di banche dati o di studi di diversi soggetti e istituzioni (ISTAT, Università e Centri di ricerca, ecc.). Particolare importanza rivestono i dati giudiziari relativi al tasso di criminalità generale del territorio di riferimento (ad esempio, omicidi, furti nelle abitazioni, scippi e borseggi), alla presenza della criminalità organizzata e/o di fenomeni di infiltrazioni di stampo mafioso nelle istituzioni, nonché più specificamente ai reati contro la pubblica amministrazione (corruzione, concussione, peculato etc.) reperibili attraverso diverse banche dati (ISTAT, Ministero di Giustizia, Corte dei Conti o Corte Suprema di Cassazione). Può essere molto utile inoltre condurre apposite indagini relative agli *stakeholder* di riferimento attraverso questionari online o altre metodologie idonee (es. focus group, interviste etc.). Mentre riguardo alle fonti interne, l’amministrazione può utilizzare interviste con l’organo di indirizzo o con i responsabili delle strutture; segnalazioni ricevute tramite il canale del *whistleblowing* o altre modalità; risultati dall’azione di monitoraggio del Rpct; informazioni raccolte nel corso di incontri e/o attività congiunte con altre amministrazioni che operano nello stesso territorio o settore, in ANAC, *Allegato 1. Indicazioni metodologiche per la gestione dei rischi corruttivi*, 2019, p. 9.

²⁵*Ibidem*.

²⁶A tal riguardo si veda FUTURE OF LIFE INSTITUTE, *Asilomar AI Principles*, 2017 (principles developed in conjunction with the 2017 Asilomar conference); J. COWLS, L. FLORIDI, *Prolegomena to a White Paper on an Ethical Framework for a Good AI Society*, 2018.

²⁷G. MISURACA, C. VAN NOORDT, *AI Watch - Artificial Intelligence in public services*, Publications Office of the European Union, 2020, JRC120399.



²⁸Tale termine si rinviene in E. CARLONI, *AI, algoritmi e pubblica amministrazione in Italia*, in “IDP: Revista de Internet, Derecho y Política”, 2019, n. 30; Inoltre, è importante in tal senso TAR Lazio, sez. III bis, 13 settembre 2019, n. 10964, nella quale si afferma che: «Il Collegio è del parere che le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l’attività cognitiva, acquisitiva e di giudizio che solo un’istruttoria affidata ad un funzionario persona fisica è in grado di svolgere».

²⁹Relativamente al difetto di motivazione e opacità dell’algoritmo, si veda R. CAVALLO PERIN, *Ragionando come se la digitalizzazione fosse data*, in “Rivista trimestrale di diritto amministrativo”, 2020, n. 2, pp. 313-317. Sulla decisione amministrativa automatizzata si veda G. FASANO, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica*, in “MediaLaws”, 2019, n. 3; R. FERRARA, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in “Diritto amministrativo”, 2019, n. 4.

³⁰Così D.-U. GALETTA, J.G. CORVALÁN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in “federalismi.it”, 2019, n. 3, p. 14.

³¹ANAC, *Pna 2012. Allegato 2: Le aree di rischio*, 2012.

³²In particolare, al comma 16 dell’art. 1.

³³In particolare la lett. b) del comma 1 sancisce: «l’utilizzo di strumenti informatici e digitali e, facoltativamente, lo svolgimento in videoconferenza della prova orale, garantendo comunque l’adozione di soluzioni tecniche che ne assicurino la pubblicità, l’identificazione dei partecipanti, la sicurezza delle comunicazioni e la loro tracciabilità, nel rispetto della normativa in materia di protezione dei dati personali e nel limite delle pertinenti risorse disponibili a legislazione vigente».

³⁴Si tratta del combinato disposto degli artt. 1, 3, 51 e 97 Cost.

³⁵In merito a ciò si veda L. IANNUCILLI, A. DE TURA (a cura di), *Il principio di buon andamento dell’amministrazione nella giurisprudenza della Corte costituzionale*, in “www.cortecostituzionale.it”, 2015.

³⁶Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

³⁷In tal merito si veda E.J. MAIER, *Advancing Artificial Intelligence and Machine Learning in the U.S. Government Through Improved Public Competitions*, in “arXiv.org”, 2021. Sulla relazione tra intelligenza artificiale, apprendimento automatico e discriminazione di genere si evincono spunti interessanti in M.T. NUSEIR, B.H. AL KURDI, M.T. ALSHURIDEH, H.M. ALZOUBI, *Gender Discrimination at Workplace: Do Artificial Intelligence (AI) and Machine Learning (ML) Have Opinions About It*, Springer, 2021.

³⁸Sulla questione della potenziale discriminazione derivante dall’IA si veda M. PERUZZI, *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in “Labour & Law Issues”, 2021, n. 1; A. SIMONCINI, *L’algoritmo incostituzionale: intelligenza artificiale e il futuro della libertà*, in “BioLaw Journal”, 2019, n. 1; I. VALENZI, *Libertà religiosa e intelligenza artificiale: prime considerazioni*, in “Quaderni di diritto e politica ecclesiastica”, 2020, n. 2; L. GIACOMELLI, *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell’intelligenza artificiale: quale tutela per il corpo digitale?*, in “BioLaw Journal”, 2019, n. 2.

³⁹«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: a) sia necessaria per la conclusione o l’esecuzione di

un contratto tra l’interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato; c) si basi sul consenso esplicito dell’interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell’interessato, almeno il diritto di ottenere l’intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all’articolo 9, paragrafo 1, a meno che non sia d’applicazione l’articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato».

⁴⁰Sul punto si vedano F. PIZZETTI (a cura di), *Intelligenza artificiale e, protezione dei dati personali e regolazione*, Giappichelli, 2018; F. LORÈ, *Una intelligenza artificiale più umana, tra etica e privacy*, in “Ciberspazio e diritto: rivista internazionale di informatica giuridica”, 2021, n. 1, pp. 165-203; T.E. FROSINI, *La privacy nell’era dell’intelligenza artificiale*, in “dpce online”, 2022, n. 1, pp. 273-284; C. CASONATO, *Costituzione e intelligenza artificiale: un’agenda per il prossimo futuro*, in “BioLaw Journal”, 2019, n. 2, pp. 711-725.

⁴¹In tal senso A. PAJNO, M. BASSINI, GI. DE GREGORIO et al., *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in “BioLaw Journal”, 2019, n. 3, p. 208.

⁴²ANAC, *Misurazione territoriale del rischio corruzione e promozione della trasparenza – Progetto PON*, 2020. Alla data di gennaio 2022 sono stati identificati ben 71 indicatori per la misurazione e il contrasto della corruzione, suddivisi in 3 aree tematiche distinte: 1. Indicatori di contesto (49 indicatori articolati in 4 ambiti – Criminalità, Istruzione, Economia e territorio, Capitale Sociale –); 2. Indicatori sugli Appalti (17 indicatori) incentrati sulla banca dati nazionale dei contratti pubblici di ANAC; 3. Indicatori “comunali” relativi ai Comuni sopra 15.000 abitanti (5 indicatori), in *Indici di misurazione della corruzione. Il progetto di Anac, dibattito con Eurispes*, webinar, gennaio 2022.

⁴³M. GNALDI, B. PONTI, *Misurare la corruzione oggi. Obiettivi, metodi, esperienze*, Franco Angeli, 2018, p. 66.

⁴⁴M. SALLES MELO LIMA, D. DELEN, *Predicting and explaining corruption across countries: A machine learning approach*, in “Government Information Quarterly”, vol. 37, 2020, n. 1; F.J. LÓPEZ-ITURRIAGA, I. PASTOR SANZ, *Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces*, Social indicators Research, Springer, 2018, pp. 975-998; L.M.C. DORIA, F.F. DORIA, P. FIGUEIREDO et al., *A Machine Learning Approach on the Problem of Corruption*, in “International Journal of Advanced Engineering Research and Science”, vol. 9, 2022, n. 3.

⁴⁵Sul tema V. FROSINI, *La protezione della riservatezza nella società informatica*, in N. Matteucci (a cura di), “Privacy e banche dei dati”, il Mulino, 1981.

⁴⁶L’art. 2 specifica che il regolamento si applica: «al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi». Sul tema si rinvia a T.E. FROSINI, *La privacy nell’era dell’intelligenza artificiale*, in “dpce online”, 2022; T.E. FROSINI, *Le sfide attuali del diritto ai dati personali*, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), “Dati e algoritmi. Diritto e diritti nella società digitale”, il Mulino, 2020; G. FINOCCHIARO, *XVIII lezione: intelligenza artificiale, privacy e data protection*, in U. Ruffolo (a cura di), “XXVI Lezioni di diritto dell’intelligenza artificiale”, Giappichelli, 2021.



⁴⁷Diffusamente sul punto si veda G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, 2018.

⁴⁸L'elaborazione di questi tre modelli si rinviene in N. KÖBIS, C. STARKE, *Artificial Intelligence as an Anti-Corruption Tool. A Conceptual Framework*, 2021, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

⁴⁹Cfr. art. 4, par. 1, n. 1.

⁵⁰Di recente è stato creato un indice di rischio relativo di corruzione in una ricerca finalizzata a valutare l'uso di algoritmi di apprendimento automatico nell'individuazione precoce della corruzione nella pubblica amministrazione, in K.M.S. MUNOZ, *Inteligencia Artificial para Detectar Corrupción en la Administración Pública Municipal de Colombia*, Documento CEDE-Estudiantes, 2021.

⁵¹È interessante, in questo senso, uno studio effettuato in due CCIA italiane in D. GALLI, G. GIACOMELLI, G. VALOTTI, *Misurazione della performance e gestione del rischio: l'utilizzo di indicatori red flag per la prevenzione della corruzione nel settore pubblico*, in "Azienda Pubblica", 2018, n. 2, pp. 147-163.

⁵²Per far ciò sono stati indicati i seguenti progetti: favorire lo *smart procurement*; interoperabilità del sistema eProc; processi di dichiarazione e verifica dei requisiti per la partecipazione agli appalti pubblici; aste digitali; CRM evoluto; ricorso a IA e *machine learning*.

⁵³*Piano Nazionale di Ripresa e Resilienza*, 2021.

⁵⁴Si segnala una recente analisi molto interessante basata su metodi tradizionali di regressione e metodi di apprendimento automatico in M. FAZEKAS, S. SBERNA, A. VANNUCCI, *The extra-legal governance of corruption: Tracing the organization of corruption in public procurement*, in "Governance", vol. 35, 2022, n. 4, pp. 1139-1161.

⁵⁵Su indicatori di rischio nel campo del *public procurement* si vedano M. FAZEKAS, I.J. TOTH, L.P. KING, *An Objective Corruption Risk Index Using Public Procurement Data*, in "European Journal on Criminal Policy and Research", 2016, n. 22, pp. 369-397; M. FAZEKAS, G. KOCSIS, *Uncovering high-level corruption: Crossnational objective corruption risk indicators using public procurement data*, in "British Journal of Political Science", vol. 50, 2020, n. 1, pp. 155-164.

⁵⁶Così A. SANCHEZ-GRAELLS, *Can artificial intelligence bring corruption in public procurement to an end?*, in "University of Bristol Law School Blog", 2021.

⁵⁷Sul sito di Cineca.it il *text mining* viene definito come una tecnica di intelligenza artificiale che utilizza l'elaborazione del linguaggio naturale per trasformare il testo libero, non strutturato in dati strutturati e normalizzati.

⁵⁸Tali ipotesi sono sostenute in K. RABUZIN, N. MODRUŠAN, *Prediction of Public Procurement Corruption Indices using Machine Learning Methods*, in J.L.G. Dietz, D. Aveiro, J. Filipe (eds.), "Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019)", Scitepress, 2019, pp. 333-340.

⁵⁹Così P. AARVIK, *Blockchain as an anticorruption tool. Case examples and introduction to the technology*, in "U4 Issue", 2020.

⁶⁰Tale termine si deve a E. CARLONI, *Il paradigma trasparenza. Amministrazioni, informazioni, democrazia*, il Mulino, 2022, p. 292.

⁶¹Al comma 5 dell'art. 1 della l. n. 179/2017 è infatti sancito che: «le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione».

⁶²GARANTEE PER LA PROTEZIONE DEI DATI PERSONALI, *Newsletter n. 488 dell'11 maggio 2022*.

⁶³Tale proposta è presente in A.E.B. TOMAZ, J.C. DO NASCIMENTO, J.N. DE SOUZA, *Blockchain-based whistleblowing service to solve the problem of journalistic conflict of interest*, in "Annals of Telecommunications", vol. 77, 2022, n. 1-2, pp. 101-118.

⁶⁴In questo senso si veda F. ODILLA, *Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology*, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

⁶⁵Una raccolta di diverse esperienze si trova in UNITED NATIONS ESCAP, *Artificial intelligence in the Delivery of Public Services. Report*, 2019.

⁶⁶Gli studiosi hanno scelto di non menzionare i casi più soggetti a corruzione per evitare polemiche.

⁶⁷F.J. LÓPEZ-ITURRIAGA, I. PASTOR SANZ, *Predicting Public Corruption with Neural Networks*, cit.

⁶⁸Relativamente al limite degli indicatori di percezione, alcuni studiosi hanno proposto di basarsi sugli *hard data* di fonte amministrativa in B. PONTI, *Oltre la percezione: concretizzare le potenzialità conoscitive degli indicatori basati sull'elaborazione degli hard data di fonte amministrativa*, in M. Gnaldi, B. Ponti (a cura di), "Misurare la corruzione oggi", cit., pp. 47-58.

⁶⁹Vantaggi e problemi derivanti da questo tipo di iniziative, in particolare dell'operazione *Serenada de amor* si riscontrano in F. ODILLA, *Citizens and their bots that sniff corruption: Using digital media to expose politicians who misuse public money*, in "ECPR General Conference", virtual event, 30 August-3 September 2021.

⁷⁰Il nome del sito è stato ispirato dal caso Toblerone, che si riferisce all'episodio in cui la popolazione svedese ha chiesto le dimissioni di un ministro per l'acquisto di una tavoletta di cioccolato Toblerone e altre spese personali con la carta aziendale.

⁷¹Sulle riforme anticorruzione successive al 2014 si veda R. NIZHNIKAU, *Love the Tender: ProZorro and Anti-Corruption Reforms after the Euromaidan Revolution*, in "Problems of Post-Communism", vol. 69, 2022, n. 2.

⁷²Su alcune stime prodotte sull'utilizzo di *ProZorro* si veda A. KOVALCHUK, C. KENNY, M. SNYDER, *Examining the Impact of E-Procurement in Ukraine*, Center for Global Development Working Paper 511, 2019.

⁷³In merito alla relazione tra legalità e decisioni amministrative si rinvia a S. CIVITARESE MATTEUCCI, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in "Diritto Pubblico", 2019, n. 1.

⁷⁴In merito a ciò si rinvia a R. CALO, D.K. CITRON, *The automated administrative law: a crisis of legitimacy*, in "Emory Law Journal", vol. 70, 2021, n. 4, pp. 799-845.

⁷⁵R. FERRARA, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in "Diritto amministrativo", 2019, n. 4, pp. 773-792; G. PESCE, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, 2020; G. MARCHIANÒ, *La legalità algoritmica nella giurisprudenza amministrativa*, in "Il diritto dell'economia", 2020, n. 3, pp. 229-258; P. FALLETTA, *Alla ricerca di un paradigma giuridico della decisione amministrativa algoritmica*, in "Amministrazione in cammino", marzo 2022.

⁷⁶Emblematica di ciò è la sentenza TAR. Lazio, sez. III bis, 13 settembre 2019, n. 10964.

⁷⁷All'interno dell'Allegato 1 del PNA 2019 recante "Indicazioni metodologiche per la gestione dei rischi corruttivi", l'ANAC rileva differenze e analogie tra il processo che porta all'adozione di un piano e un procedimento amministrativo vero e proprio, nel quale si afferma che: «Un processo può essere definito come una sequenza di attività interrelate ed interagenti che trasformano delle risorse in un output destinato ad un soggetto interno o esterno all'amministrazione (utente). Si tratta di un concetto organizzativo che – ai fini dell'analisi



del rischio – ha il vantaggio di essere più flessibile, gestibile, completo e concreto nella descrizione delle attività rispetto al procedimento amministrativo».

⁷⁸Nel quale si legge che l'allegato dev'essere considerato come: «l'unico documento metodologico da seguire nella predisposizione dei Piani triennali della prevenzione della corruzione e della trasparenza (Ptpct) per la parte relativa alla gestione del rischio corruttivo».

⁷⁹Così F. DONATI, *Intelligenza artificiale e giustizia*, in "Rivista AIC", 2020, n. 1, p. 422.

⁸⁰Tale concetto è centrale in MINISTERO DELLA SALUTE - DIREZIONE GENERALE DELLA PREVENZIONE SANITARIA, *Piano Nazionale della prevenzione 2020-2025*.

⁸¹Sulla relazione input-output e IA si veda su tutti F. PASQUALE, *Black box society. The secret algorithms that control money and information*, Harvard University Press, 2015.

⁸²Anche in questo caso vi sono chiare similitudini con la disciplina sul procedimento amministrativo: partecipazione al procedimento (art. 7 e s., l. 7 agosto 1990, n. 241), diritto di accesso dei partecipi agli atti, di presentare memorie e documenti (art. 10, l. 7 agosto 1990, n. 241).

⁸³Per es. per l'invio delle proposte per l'ospedale policlinico San Martino del SSR Liguria viene dato questo indirizzo: responsabile.trasparenza@hsanmartino.it; il Rpct dell'Agcom fornisce questo indirizzo mail: agcom@cert.agcom.it; Per la revisione del codice di comportamento interno, il comune di Palermo ha indicato il seguente indirizzo mail: anticorruzione@comune.palermo.it.

⁸⁴Su cittadinanza amministrativa e buona amministrazione A. BARTOLINI, A. PIOGGIA, *Le cittadinanze amministrative,*

percorsi e prospettive dell'amministrazione tra diritti e doveri a 150 anni dalle leggi di unificazione amministrativa, in L. Ferrara, D. Sorace (a cura di), "A 150 anni dall'unificazione amministrativa italiana", Firenze University Press, 2016, pp. 9-56.

⁸⁵Si veda in tal senso C. BENETAZZO, *Intelligenza artificiale e nuove forme di interazione tra cittadino e pubblica amministrazione*, in "federalismi.it", 2020, n. 16.

⁸⁶Si veda la sezione 13 "Partecipazione" di OECD, *Oecd Public Integrity Handbook*, in "Oecd-ilibrary.org", 2020.

⁸⁷In merito ai potenziali rischi derivanti dall'impiego top-down delle tecniche di intelligenza artificiale si veda N. KÖBIS, C. STARKE, I. RAHWAN, *The promise and perils of using artificial intelligence to fight corruption*, in "Nature Machine Intelligence", 2022, n. 4, pp. 418-424.

⁸⁸Anche l'attuale proposta Europa dell'*AI Act* afferma che: «il presente regolamento non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche», in *Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica di alcuni atti legislativi dell'Unione*, COM/2021/206 final, del 21 aprile 2021, p. 30.

⁸⁹Concetto elaborato in L. FLORIDI, J. COWLS, M. BELTRAMETTI et al., *AI4People-An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in "Minds and Machines", 2018, n. 28, pp. 689-707.

* * *

Legality, algorithms and corruption: can AI techniques be used *in* and *for* the corruption prevention system?

Abstract: The article aims to consider what could be the potential opportunities and risks related to the use of artificial intelligence (AI) techniques in the Italian system of corruption prevention. In particular, it considers the risk management process, as a crucial moment for the adoption of administrative measures for the corruption prevention. The use of AI techniques could improve these phases, speed up the procedure and guarantee greater impartiality in the choice of measures. At the same time, however, the adoption of partial or total AI techniques would bring with it both certain complicated elements and a significant downsizing of the current system. An additional consideration is directed to those areas or instruments that, although not to be considered as strictly internal to the prevention system, could contribute to the preventive cause itself. The final section discusses the problematic aspects that the application of AI in the field of prevention could entail in terms of participation and legality.

Keywords: Artificial intelligence – Corruption prevention – Legality – Participation