L'Intelligenza Artificiale a supporto dei procedimenti decisionali pubblici: brevi considerazioni sul quadro normativo di riferimento in materia di protezione dei dati personali

Vincenzo Tomasello

netforLegaL - Studio Legale, Viale Coni Zugna n. 5, 20144 – Milano (MI)

Abstract

A quali condizioni ed entro quali limiti è possibile utilizzare l'Intelligenza Artificiale nel settore pubblico per fini di indirizzo e normazione (elaborazione dei testi delle iniziative e degli atti governativi e legislativi), quando essa attinge a dati personali? Breve disamina sulle principali aree di indagine e di criticità, nonché sul quadro normativo di riferimento all'interno del quale le istituzioni che intendono integrare sistemi algoritmici a supporto dei procedimenti decisionali pubblici devono sapersi orientare.

1. Introduzione

Le istituzioni pubbliche sono ormai sempre più consapevoli dei benefici che un utilizzo strategico e responsabile dei sistemi di Intelligenza Artificiale è in grado di determinare sia in termini di semplificazione dell'azione amministrativa che per generare un prezioso bacino di conoscenza al servizio delle attività di governo.

La implementazione di sistemi algoritmici nel settore pubblico può costituire, in tal senso, un fattore determinante per snellire le diverse fasi del procedimento amministrativo e per supportare gli organi decisori nelle attività di programmazione, definizione, attuazione e monitoraggio delle politiche nazionali e regionali (sulla base della ripartizione di competenze stabilita dall'art. 117 Cost.).

Rispetto al settore privato, le organizzazioni pubbliche devono affrontare una serie di sfide peculiari, prevalentemente legate alle modalità procedimentalizzate di formazione della volontà politica e amministrativa, all'ampio bacino di soggetti coinvolti, alle caratteristiche (quantitative e qualitative) delle informazioni trattate nonché alle elevate aspettative dei cittadini in merito alla trasparenza delle logiche utilizzate.

L'intelligenza artificiale applicata al settore pubblico può potenzialmente supportare enti e istituzioni in due macro-categorie di ambiti:

- da un lato, nelle attività di accertamento di situazioni giuridiche soggettive e nell'azione amministrativa di tipo provvedimentale che potrebbe (*rectius*, dovrebbe) essere interamente digitalizzata;
- dall'altro, nelle attività di programmazione, definizione, attuazione e monitoraggio delle iniziative e degli atti governativi e legislativi (nazionali e regionali).

Sul primo versante, sembra indubbio che l'utilizzazione dell'IA nella fase istruttoria possa apportare un contributo notevole all'azione amministrativa, in termini di velocizzazione e approfondimento del merito delle questioni sottese all'adozione del provvedimento.

Ma è sul fronte della produzione degli atti di programmazione politica e della normazione che il ricorso agli algoritmi potrebbe essere ancora più pregnante e strategico, grazie alla capacità di incidenza che l'IA sarebbe in grado di avere sulla fase preparatoria e, conseguentemente, sulla qualità degli atti di indirizzo e dei testi normativi.

Considerato che le istituzioni governative e legislative godono di ambiti di autonomia e discrezionalità di gran lunga più ampi rispetto alla *mera* attività amministrativa, all'aumentare del livello di responsabilità decisionale corrisponde una maggiore necessità di elaborare informazioni adeguatamente affidabili da offrire a supporto degli atti riservati alla competenza dei decisori politici.

L'utilizzo dell'IA potrebbe, in tal senso, agevolare la ricostruzione dei dati fattuali e dello stato dell'arte della materia da regolare, offrendo un contributo significativo soprattutto nei settori a elevata complessità tecnica e scientifica. Ed è su questi aspetti che focalizzeremo i passaggi successivi.

2. Quadro normativo frammentato e centralità della protezione dei dati personali

Tra i diversi fattori che ad oggi limitano l'adozione dell'intelligenza artificiale, in generale e con particolare riferimento al settore pubblico, si rileva anche l'incertezza giuridica generata da una cornice normativa tutt'altro che limpida. Sotto questo aspetto, la *legalità* – intesa come il rispetto di leggi e regolamenti applicabili – costituisce, insieme alla eticità e alla robustezza da un punto di vista tecnico, una delle componenti sulle quali deve fondarsi l'affidabilità di un sistema di IA[1].

Il tentativo degli ultimi anni di regolare un fenomeno così complesso ha dato luogo a una sovrapproduzione normativa da parte di numerosi organismi e istituzioni[2] – soprattutto attraverso testi di *soft law* diversamente denominati – delineando uno scenario caratterizzato da una pluralità di fonti, tra le quali i soggetti che applicano (o intendono applicare) tecnologie di IA devono sapersi orientare.

L'approccio "antropocentrico" e il rimando a principi e ad elementi valoriali – che pure sembrerebbe necessario in virtù dell'incessante ritmo del progresso tecnologico – rischiano di rendere la disciplina quasi *evanescente*, poco chiara nel definire cosa si può fare e a quali condizioni, creando di fatto moltissime incertezze per gli operatori chiamati alla loro applicazione.

Nel caso di specie, oggetto delle analisi algoritmiche è il "patrimonio informativo" pubblico, prevalentemente costituito da dati personali di cittadini tra cui, sovente, rientrano anche i dati "particolari" – quelli afferenti alla sfera più intima e privata degli individui – per i quali, salvo limitate eccezioni individuate dalla legge, la regola generale prevede il divieto di trattamento[3].

La normativa a protezione dei dati personali è dunque una delle aree giuridiche più impattanti sulla concreta fattibilità di progetti di utilizzo dell'intelligenza artificiale nel settore pubblico, imponendo alle istituzioni che intendano integrare le logiche algoritmiche a supporto dei procedimenti decisionali di tenere in debita considerazione il complesso quadro regolatorio venutosi a delineare.

In questo contesto, il Regolamento UE 2016/679[4] si pone come il riferimento normativo primario, sebbene la sua natura "tecnologicamente neutra" impedisca riferimenti espliciti a *big data* e *intelligenza artificiale* facendo spesso emergere, nella pratica, uno scarto tra il precetto normativo e le nuove fattispecie di trattamento costantemente in evoluzione.

Nel GDPR, il bilanciamento tra interesse pubblico e protezione dei dati personali è certamente presente e ben declinato. Tuttavia, il trattamento di dati personali per finalità di ricerca (statistica o scientifica) segue un percorso più chiaro e definito rispetto ai trattamenti effettuati per motivi di indirizzo e normazione delle iniziative e degli atti pubblici. È come se il GDPR facesse un passo indietro rispetto alla sovranità degli Stati membri, rimettendo alle scelte compiute dai legislatori nazionali la definizione del quadro regolatorio sull'utilizzabilità di dati personali per alimentare sistemi di intelligenza artificiale nel settore pubblico.

In Italia, la partita si gioca sul coordinamento delle regole europee con il Codice Privacy[5] e con atti normativi emanati a livello nazionale e regionale, amplificando il grado di complessità nella individuazione dei percorsi di *compliance* che le istituzioni sono tenute a seguire.

3. Regole e principi del GDPR per i trattamenti automatizzati: cenni sulle principali aree di indagine e criticità

Affrontando il tema degli algoritmi applicati ai processi decisionali pubblici, uno dei principi cardine da considerare è quello enunciato dall'art. 22 del GDPR, consistente nel diritto degli interessati di non essere sottoposti a decisioni basate *unicamente* su trattamenti automatizzati che producano effetti giuridicamente rilevanti o, comunque, parimenti significativi sulla propria sfera individuale. Questa considerazione rende ancora più evidente come la digitalizzazione dell'azione pubblica, in tutte le sue fasi, non può prescindere dall'intervento umano per le dovute valutazioni di contesto, visione e prospettiva degli interessi in gioco, a presidio del sistema costituzionale di libertà e di democrazia.

Più che raccogliere dati da destinare alle analisi e all'addestramento degli algoritmi, la grande sfida per il settore pubblico consiste – specie per i fini considerati – nel valorizzare ed estrarre conoscenza dai grandi archivi di dati già a disposizione delle istituzioni.

Secondo il GDPR, questa tipologia di attività – prevedendo l'uso di *nuove tecnologie*,

considerata la natura, l'oggetto, il contesto e le finalità del trattamento – è in grado di presentare un rischio potenzialmente elevato per i diritti e le libertà delle persone fisiche coinvolte nelle analisi, imponendo al titolare, prima di procedere al trattamento, di effettuare una *valutazione di impatto*[6].

Una prima area di approfondimento in questa valutazione riguarda il tema della praticabilità del cd. *secondary use* dei dati personali per finalità che, secondo il disposto normativo[7], non devono risultare incompatibili rispetto a quelle della raccolta originaria (in occasione della quale gli interessati dovrebbero avere già ricevuto le dovute informazioni).

A questa indispensabile analisi preliminare di compatibilità – necessario contraltare per il rispetto del principio di finalità – seguono specifichi obblighi in termini di trasparenza e informazione, diversificati sulla base della circostanza che i dati vengano acquisiti direttamente o indirettamente (tramite, ad esempio, comunicazione da parte di un'altra PA) dal soggetto pubblico che intende effettuare le analisi[8].

Oltre alla estrema complessità nell'individuare con esattezza l'origine dei dati nel *mare magnum* dei grandi archivi pubblici, gli obblighi informativi a carico del Titolare del trattamento nei casi di acquisizione diretta potrebbero risultare – stando al dettato normativo – particolarmente complessi (financo *abnormi*) da realizzare per quanto attiene al principio di trasparenza, rischiando di tradursi in un dovere di informativa *one to one* verso ciascun cittadino coinvolto nelle analisi.

Una seconda area di indagine riguarda la corretta individuazione della *base giuridica*, anche in considerazione del rischio – intrinsecamente legato alle nuove frontiere dell'IA – che la tradizionale distinzione tra dati sensibili e non venga a sfumare nel mondo dei *big data* (specie nei casi di incrocio tra dati custoditi in archivi differenti).

Per evitare di cadere in zone grigie, il cui perimetro viene amplificato dagli ulteriori e connessi rischi di *inferenza* e *reidentificazione*, è auspicabile che l'atto giuridico posto a fondamento delle analisi di dati (anche personali) effettuate con soluzioni di *big data* disciplini dettagliatamente i motivi di interesse pubblico rilevante, le tipologie di dati che possono costituire oggetto di trattamento, le operazioni eseguibili nonché le misure appropriate e specifiche per tutelare i diritti fondamentali degli interessati[9].

Per quanto l'utilizzo dei *big data* e delle tecniche algoritmiche renda sempre più complesso identificare una netta linea di demarcazione tra dati personali, dati non personali e dati anonimi, il tema della distinzione tra questi *insiemi* diventa centrale al fine di stabilire a monte (e durante tutto il processo di analisi) le misure tecniche e organizzative adeguate per mitigare i potenziali impatti negativi sui diritti e sulle libertà degli individui.

In linea generale, il principio che sembra maggiormente interpretare l'esigenza di integrare il rispetto dei diritti fondamentali nello sviluppo tecnologico è quello della *privacy by design* sancito dall'art. 25 del GDPR che, arricchito dalla componente valoriale formulata nel Considerando 78, rende la norma un precetto dal tenore *quasi costituzionale*[10].

In mancanza di regole specifiche sia nel GDPR che nella legislazione nazionale, la progettazione assume dunque un ruolo centrale insieme a un altro principio cardine del GDPR, quello dell'*accountability* (nella sua doppia accezione di responsabilizzazione e di rendicontazione), spostando il baricentro sulla crucialità di un modello di governance che renda "dimostrabile" – specie nei confronti dei cittadini – il presidio dell'intero ciclo di vita delle analisi (dalla raccolta dei dati fino alla estrazione di conoscenza e all'utilizzo).

La trasparenza dei processi e delle logiche utilizzate rappresenta, secondo questa lettura, un fattore chiave il cui perseguimento deve essere considerato più che mai irrinunciabile.

4. Conclusioni

Alla domanda "a quali condizioni ed entro quali limiti è possibile usare l'intelligenza artificiale nel settore pubblico per fini di indirizzo e normazione, quando essa attinge a dati personali?", non è possibile rispondere in modo univoco. Esistono principi e meccanismi del GDPR, norme di livello alto nel Codice Privacy, unitamente ad una potestà normativa istituzionalmente riservata ai diversi soggetti pubblici che si avvarrebbero dei sistemi stessi.

L'assenza di regole e procedure predefinite per lo svolgimento di analisi *avanzate* da parte delle istituzioni pubbliche non preclude che esse vengano svolte. Occorre, tuttavia, interpretare le regole e i principi del GDPR, attuare alcune

norme del nostro ordinamento nazionale, individuare il percorso appropriato. In questa delicata opera di composizione, risalta la centralità della *privacy by design* e dei relativi modelli di *governance*.

Per consentire all'intelligenza artificiale di dispiegare a pieno i propri effetti positivi sui singoli e sulla collettività attraverso queste applicazioni pionieristiche della tecnologia, il decisore pubblico è tenuto a cogliere questa opportunità analizzando i rischi per i diritti e le libertà delle persone, valorizzando (ed inverando) il principio di *accountability* nella valutazione e documentazione della proporzionalità dei trattamenti, regolamentando il trattamento con appositi atti normativi e consultando il Garante nei casi in cui ciò si renda necessario.

Le capacità conoscitive al servizio del decisore politico possono essere rafforzate – in linea con l'egregio e prezioso compito svolto ormai da anni dalle strutture tecniche di supporto legislative e governative – solo dopo aver messo a fuoco le tappe dell'iter che i soggetti pubblici devono seguire, ai sensi della normativa a protezione dei dati personali, se intendono integrare sistemi di intelligenza artificiale nei procedimenti decisionali. Queste imprescindibili premesse permetterebbero un cambio di passo per garantire traguardi più efficaci di fattibilità delle norme a tutto vantaggio della società nel suo complesso.

5. References

[1] Gruppo indipendente di esperti di alto livello sull'IA istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per una intelligenza artificiale affidabile*, 8 aprile 2019.

[2] Oltre agli Orientamenti sopra richiamati, si citano, tra le principali: OCSE (Organizzazione per la cooperazione e lo sviluppo economico), *Linee guida relative ai principi sull'intelligenza artificiale*, 22 maggio 2019; Raccomandazione del Consiglio d'Europa, *Unboxing Artificial Intelligence: 10 steps to protect human rights*, 14 maggio 2019; Commissione Europea, *Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020; da ultimo, la proposta di Regolamento UE del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 21 aprile 2021, oltre a una serie di Risoluzioni del Parlamento europeo sul tema (Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale; Risoluzione del Parlamento europeo del 6 ottobre 2021 sull'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale; Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale).

[3] Si veda, sul punto, l'art. 9 del Regolamento UE 2016/679.

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[5] D.lgs. 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 […]".

[6] Secondo l'art. 35.1 del GDPR, "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali […]".

[7] Si veda, in tal senso, il principio di finalità enunciato dall'art. 5.1, lett. *b*) del GDPR, nonché la enucleazione degli elementi – nei casi indicati dall'art. 6.4 del GDPR – che il titolare è tenuto a considerare, tra gli altri, qualora decida di effettuare trattamenti per una finalità diversa da quella per la quale i dati personali sono stati originariamente raccolti.

[8] Nel primo caso, si applica – in termini di contenuto dell'informativa e di modalità per veicolarla – l'art. 13 del GDPR (*Dati personali raccolti presso l'interessato: informazioni da fornire*); nel secondo, invece, trova applicazione l'art. 14 del GDPR (*Dati personali non ottenuti presso l'interessato: informazioni da fornire*).

[9] Sul punto, si segnala come il DL 8 ottobre 2021 n. 139, convertito, con modificazioni, dalla legge 3 dicembre 2021 n. 205 (cd. "Decreto Capienze"), ha modificato gli artt. 2-*ter* e 2-*sexies* del Codice Privacy introducendo la previsione di una nuova base giuridica per il trattamento dei dati personali comuni e "particolari" costituita dagli "atti amministrativi generali", nonché la possibilità per le pubbliche amministrazioni di trattare i dati personali se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti.

[10] Si veda l'intervento di Ginevra Cerrina Feroni, vice Presidente del Garante per la protezione dei dati personali, del 14 febbraio 2023, *Intelligenza artificiale e ruolo della protezione dei dati personali*.