Consultazione pubblica nell'ambito della "Bozza di linee guida per l'adozione di IA nella pubblica amministrazione", ai sensi del DPCM 12 gennaio 2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026".

Contributo di Himmel Advisors

Himmel Advisors S.r.l.

Il legittimo interesse: sistemi di IA e PA

Negli ultimi mesi, il dibattito si è acceso attorno alla questione della liceità dell'uso dei sistemi di IA nell'ambito della Pubblica Amministrazione. Questo fervore deriva dalla comprensibile preoccupazione che l'impiego di tali sistemi possa comportare, seppur non necessariamente, il trattamento illegittimo di dati personali. Ne consegue – per alcuni – che l'implementazione di simili tecnologie deve essere sorretta da una solida base giuridica, in grado di legittimarne l'uso, soprattutto nel settore pubblico.

In questo contesto, il legittimo interesse assume un ruolo di primaria importanza, divenendo – anche erroneamente – la base giuridica prescelta per giustificare l'adozione e l'operatività di sistemi di IA. Tale base giuridica si erge a pilastro, applicabile in modo uniforme e senza distinzioni all'interno del complesso panorama normativo in cui si colloca. Tuttavia, si ritiene fondamentale, dunque, che le autorità competenti e gli operatori del settore considerino attentamente le implicazioni etiche, giuridiche e sociali di questo approccio, affinché l'innovazione tecnologica possa realizzarsi in armonia con i principi fondamentali di protezione dei dati e dei diritti dei cittadini.

A tale proposito è bene ricordare che l'interesse legittimo è uno dei fondamenti di liceità per il trattamento dei dati personali previsto dal Regolamento (UE) 2016/679, di seguito, anche GDPR). Tale base giuridica si applica "quando il trattamento dei dati è necessario per perseguire un legittimo interesse del titolare del trattamento o di un terzo, a condizione che su tale interesse non prevalgano i diritti e le libertà fondamentali dell'interessato, in particolare se l'interessato è un minore" (art. 6, comma 1 lett. f) GDPR).

Tuttavia, è doveroso ricordare che la base giuridica del legittimo interesse – come stabilito al comma 1 dell'art. 6 del GDPR, "non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti". Così viene ribadito nel considerando 47 del medesimo Regolamento che stabilisce "[p]osto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti".

Il dubbio circa la base giuridica applicabile all'impiego dell'intelligenza artificiale appare, in verità, piuttosto superficiale. Infatti, i più significativi atti giuridici vincolanti applicabili, quali il Regolamento (UE) 2016/679 e, in particolare, il Regolamento (UE) 1689/2024 (c.d. AI Act), non forniscono riferimenti chiari riguardo alla base giuridica da applicare nell'ambito dell'utilizzo di tali sistemi da parte delle PA. È evidente che tali normative non legittimano le pubbliche amministrazioni, in qualità di Titolari del trattamento (deployer), ad avvalersi del legittimo interesse quale fondamento giuridico per le proprie operazioni di trattamento. Questa constatazione è cruciale, poiché implica che le attività di trattamento condotte dalle PA debbano necessariamente ruotare attorno a basi giuridiche diverse, adeguatamente contemplate dalla normativa vigente, nel rispetto dei diritti e delle libertà fondamentali dei cittadini; nello specifico "l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6 comma 1 lett. e) GDPR).

In questo senso, è imperativo che il quadro normativo venga interpretato con rigore e precisione, anche attraverso l'impiego di linee guida operative, affinché l'innovazione tecnologica non comprometta la tutela dei dati personali e la fiducia dei cittadini nelle istituzioni pubbliche.

È fondamentale sottolineare che un sistema di IA non deve essere assimilato a un'attività di trattamento, ma si configura piuttosto come "un sistema automatizzato progettato per operare con livelli di autonomia variabili, in grado di manifestare adattabilità anche dopo la sua diffusione. Esso, per obiettivi espliciti o impliciti, deduce dall'input ricevuto come generare output, quali previsioni, contenuti, raccomandazioni o decisioni, con la potenziale capacità di influenzare ambienti fisici o virtuali" (art. 3 AI Act).

A tale riguardo, appare chiaro che il legislatore non ha il compito di individuare la base giuridica applicabile all'utilizzo di tali sistemi, ma piuttosto di imporre ai Titolari del trattamento l'obbligo di identificare la base giuridica appropriata per le operazioni di trattamento associate all'impiego dell'IA. Questa responsabilità conferisce un'importante dimensione di autonomia e di consapevolezza ai Titolari, i quali devono affrontare sfide normative e garantire che le loro pratiche siano sempre allineate con le previsioni giuridiche vigenti, tutelando nel contempo i diritti e le libertà dei soggetti coinvolti.

Una cosa è chiara: le pubbliche amministrazioni non possono legittimare le proprie attività di trattamento in cui viene utilizzato un sistema di IA basandosi sul legittimo interesse.

Nel campo dell'IA, la necessità di determinazione e l'ambito di applicazione della base legittimante di tali sistemi è stato oggetto di vari approfondimenti e interpretazioni sia da parte delle autorità di protezione dati dei singoli Stati membri dell'UE, sia da parte dell'EDPB (s.v. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024).

La bozza di linee guida proposta dall'AGID (di seguito, anche "bozza di linee guida") manca di qualsiasi riferimento alla base giuridica applicabile in merito all'utilizzo di un sistema di intelligenza artificiale, rinviando al Parere sopra menzionato, dove viene approfondito il tema dell'"adeguatezza dell'interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto dello sviluppo e dell'implementazione dei modelli di IA e il possibile impatto di un trattamento illecito di dati personali".

Tale Parere, infatti, ricorda che "non esiste una gerarchia tra le basi giuridiche fornite dal GDPR" e che "spetta ai titolari del trattamento identificare la base giuridica appropriata per le loro attività di trattamento". Tuttavia, dall'applicazione di questo principio deve essere esclusa la base giuridica dell'interesse legittimo in quanto non applicabile alle PA.

Pertanto, è responsabilità della PA condurre il cosiddetto *necessity test* o analisi di rischi allo scopo di valutare preventivamente, in virtù del meta-principio di "AI by design" e "by default", se il sistema di IA utilizzato per il trattamento in oggetto (a) sia necessario al fine di raggiungere l'obiettivo prefissato e (b) se esistano alternative meno invasive per conseguire il medesimo obiettivo. Questa analisi preliminare è essenziale per garantire che l'adozione delle nuove tecnologie avvenga nel pieno rispetto dei diritti e delle libertà dei cittadini, mitigando al contempo i rischi inerenti al trattamento dei dati personali.

Queste interpretazioni – rivolte al settore privato – mirano a "chiarire" le condizioni e i limiti entro cui l'interesse legittimo può essere invocato, sottolineando la necessità di un attento bilanciamento tra l'interesse legittimo perseguito dal titolare del trattamento (soggetto privato) o dal terzo e i diritti e le libertà fondamentali dell'interessato/a.

Per tutto quanto sopra premesso, si suggerisce di modificare la "bozza di linee guida" per evitare ambiguità e garantire che le disposizioni ivi presenti siano pienamente conformi agli obiettivi stabiliti, nonché coerenti con le normative applicabili. In particolare, si raccomanda di esplicitare chiaramente che, nel contesto della PA, il legittimo interesse non può essere considerato una base giuridica valida (Paragrafo n. 4, pagina 66 della "bozza di linee guida"). Tale precisazione è essenziale per assicurare che le linee guida, a seguito dell'approvazione da parte dell'AGID, riflettano con precisione le limitazioni normative vigenti e guidino correttamente le pratiche delle PA nel trattamento dei dati mediante l'uso di sistemi di IA a norma.

Governance

La “bozza di linee guida” fornisce un riferimento interessante ed esaustivo alla terminologia utilizzata nel documento, illustrando chiaramente il dovere, l’obbligo e la facoltà delle disposizioni rivolte alla PA che intendono avvalersi di sistemi di IA.

Tuttavia, per quanto riguarda la sezione “Governance”, è degno di nota come sia stato indicato come “dovere” ciò che, in realtà, si configura come un vero e proprio “obbligo”.

In particolare, ci si riferisce alla definizione e all’adozione di “procedure di governance per lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale”. Questa distinzione terminologica è cruciale, in quanto l’adozione formale di procedure di governance non è una mera facoltà, ma un requisito necessario per garantire che l’ideazione, lo sviluppo e l’applicazione di sistemi di IA avvengano in conformità con i principi stabiliti dalla vigente normativa e in maniera responsabile.

Come si evince dall’AI Act, l’adozione di procedure di Governance per lo sviluppo e, in particolare, per l’utilizzo dei sistemi di IA non costituisce un semplice dovere per il deployer (e ancor più nel caso delle PA), ma rappresenta un vero e proprio obbligo, in virtù del principio di accountability (responsabilità delle organizzazioni nel dimostrare la conformità normativa).

L’obbligo di strutturazione e adozione di procedure interne relative all’uso dell’IA non solo consentirebbe alle PA di definire chiaramente il modus operandi, le misure di sicurezza tecniche ed organizzative e le garanzie a supporto fin dalla progettazione e per impostazione predefinita, i settori e le pratiche vietate, ma le metterebbe anche in condizione di dimostrare all’autorità competente le modalità di impiego dei sistemi di IA. Questo processo non solo rafforza la trasparenza, la conformità normativa e la certezza giuridica nei confronti dei cittadini, ma promuove anche un utilizzo etico e responsabile delle tecnologie emergenti, allineandosi con gli alti standard di tutela previsti dal Codice dell’Amministrazione Digitale (CAD).

La propria “bozza di linee guida” specificano che “[f]ermi restando gli obblighi di conformità all’AI Act, le PA DEVONO adottare un codice etico per l’IA. Tale codice DEVE divenire uno strumento di governance vincolante, allineato con il quadro normativo vigente, integrato nei processi decisionali e operativi della PA, finalizzato a un uso responsabile, equo e trasparente dell’IA”. È inoltre da considerare come, al punto 4.9 della suddetta “bozza di linee guida”, si dice che “la PA DEVE adottare un approccio sistematico e documentato di project management definendo un piano operativo”. In effetti, “Il piano operativo DEVE includere tutte le attività necessarie per il conseguimento degli obiettivi riguardanti la gestione (cfr. presenti Linee guida), il procurement (cfr. Linee guida per il procurement dell’IA), lo sviluppo (cfr. Linee guida per lo sviluppo dell’IA) dei sistemi di IA adottati o adottandi dalla PA”.

In questo senso, si suggerisce di rivedere l'affermazione per rendere “obbligatoria” l'adozione di procedure di governance per lo sviluppo e l’utilizzo dei sistemi di IA come un vero obbligo per le PA. Di conseguenza, la formulazione dovrebbe essere così modificata: "La PA DEVE definire procedure di governance per lo sviluppo e l'utilizzo dei sistemi di IA. Tali procedure DEVONO essere coerenti con la strategia per l'IA dell’ente e con la strategia definita nel PIAO." Questo cambiamento terminologico sottolinea l'importanza di un impegno formale nella gestione e implementazione dei sistemi di IA, rafforzando il rispetto delle normative e promuovendo un uso responsabile e strategico delle tecnologie emergenti all'interno delle istituzioni pubbliche.

Valutazione di impatto

Relativamente all’obbligo di effettuare una “valutazione di impatto”, dal punto di vista prettamente grammaticale, si suggerisce di inserire la dicitura completa da cui derivano le iniziali FRIA, che in inglese è "Fundamental Rights Impact Assessment" (FRIA). Lo stesso suggerimento vale per quanto concerne la DPIA. È consigliabile includere queste diciture complete sia nel glossario, per completezza, sia nel testo, oppure, per comodità, esclusivamente nel glossario. Questo accorgimento contribuirà a garantire chiarezza e comprensione uniformi, facilitando la consultazione e la corretta applicazione delle linee guida da parte di tutti gli attori coinvolti nel processo normativo e operativo.

Dal punto di vista operativo, sebbene la "bozza di linee guida" rappresenti un progresso verso la compliance normativa, in merito all'obbligo di effettuare una valutazione preventiva per determinare il tipo di rischio associato all'uso di un sistema di intelligenza artificiale, si ritiene opportuno stabilire che il processo di valutazione delle potenziali conseguenze sui diritti fondamentali, derivanti dallo sviluppo, utilizzo o uso improprio di tali sistemi, anche quando si tratti di sistemi IA a "rischio minimo o nessun rischio", diventi un obbligo.

È importante distinguere tra l'obbligo di effettuare la valutazione e la procedimentalizzazione di tale obbligo. In altre parole, dovrebbe essere obbligatorio definire, all'interno della propria procedura, quando effettuare la DPIA (Data Protection Impact Assessment) e la FRIA (Fundamental Rights Impact Assessment), previa un'analisi dei rischi. Come delineato nella "bozza di linee guida", "resta ferma la necessità di svolgere la valutazione del rischio sulla protezione dei dati personali nelle attività istituzionali e progettuali condotte mediante strumenti di IA, ai sensi della normativa vigente e dei provvedimenti del Garante per la protezione dei dati personali (cfr. Cap. 10)". È fondamentale ricordare che non si tratta di una semplice "necessità", ma di un vero e proprio obbligo che ricade sul titolare del trattamento (PA). Questa distinzione rafforza l'importanza di un approccio sistematico e predefinito, volto a garantire il rispetto dei diritti fondamentali e delle normative vigenti nel contesto dell'adozione tecnologica avanzata.

A tale scopo si ritiene opportuno, qualora non sia necessaria l'effettuazione di una DPIA e FRIA in quanto il rischio risulti medio o inesistente, fornire una motivazione approfondita da parte del deployer che spieghi perché non ha ritenuto necessario procedere, successivamente, con una DPIA e FRIA. Tale evidenza è fondamentale per dimostrare la consapevolezza e l'attenzione riposta nella valutazione dei rischi potenziali, assicurando trasparenza e accountability nel processo decisionale. Tale requisito consentirebbe di consolidare ulteriormente la fiducia delle autorità e del pubblico nell'operato dei titolari del trattamento e dei deployer, garantendo al contempo il pieno rispetto delle normative vigenti.

Un altro aspetto non sufficientemente considerato nella "bozza di linee guida" è che, ai sensi del comma 4 dell'art. 27 dell'AI Act, "[s]e uno qualsiasi degli obblighi di cui all'art. 27 è già rispettato mediante la [DPIA] effettuata a norma dell'art. 35 del [GDPR] o dell'articolo 27 della Direttiva (UE) 2016/680, la [FRIA] integra tale [DPIA]".

Questo implica che, laddove le DPIA siano già state eseguite nell'ambito del medesimo trattamento e soddisfino i requisiti previsti, la FRIA può essere utilizzata come integrazione e approfondimento delle considerazioni già esistenti, ma non necessariamente sostitutiva. Ciò non solo ottimizza il processo valutativo, evitando la duplicazione degli sforzi, ma assicura anche un approccio coerente e comprensivo al trattamento dei dati e alla protezione dei diritti fondamentali, sottolineando l'importanza di un'integrazione normativa efficace tra diverse disposizioni legislative.

Si afferma, inoltre, che "[i] risultati della valutazione d'impatto DEVONO essere condivisi con le parti interessate", mentre nella normativa di riferimento non viene esplicitamente sancito tale obbligo, bensì viene sottolineata la necessità di coinvolgere i "soggetti interessati" durante la fase di svolgimento della DPIA ed eventualmente la FRIA. È di cruciale importanza che le parti interessate siano coinvolte attivamente "durante" lo svolgimento delle valutazioni d'impatto piuttosto che "ex post".

Coinvolgere le parti interessate lungo il percorso valutativo arricchisce il processo decisionale e permette di rispondere alla domanda più importante: è opportuno, possibile e necessario avvalersi di un sistema di IA? Tale approccio permetterebbe un confronto costruttivo e iterativo tra gli interessati in grado di anticipare e risolvere potenziali criticità prima che si giunga a una decisione finale ovvero prima di utilizzare un sistema di IA. Questo approccio consente, inoltre, di instaurare un iter valutativo e procedimentale autentico, partecipato e trasparente, evitando che le persone interessate si trovino a dover accettare passivamente una decisione già adottata. Inserire il coinvolgimento anticipato delle parti interessate nel processo valutativo (ovvero durante la conduzione della DPIA e della FRIA) assicura che le scelte siano informate e ben fondate, rispettando il principio di trasparenza e promuovendo la fiducia nel trattamento equo e responsabile dei dati personali.

Infine, riteniamo che la bozza di linee guida proposta dall'AGID e, in particolare, il "Modello di codice etico" allegato (p. 92 e ss.) rappresentino strumenti fondamentali per orientare le pubbliche amministrazioni che intendono avvalersi di un sistemi di IA.

Questi strumenti sono cruciali nel garantire che l'adozione delle tecnologie non comprometta né metta a repentaglio la libertà e i diritti fondamentali degli individui coinvolti ma, allo stesso tempo, sono necessari per tutelare le pubbliche amministrazioni.

A chiusura delle nostre considerazioni, è essenziale comprendere che le tecnologie emergenti, sebbene potenti e promettenti, esigono un approccio vigile e responsabile. Le norme, i principi etici e le valutazioni d'impatto non sono meri adempimenti burocratici, ma elementi essenziali di un movimento verso un futuro in cui l'innovazione cammina mano nella mano con i diritti umani e la dignità individuale. Le amministrazioni pubbliche sono chiamate a essere non solo custodi dei dati personali dei cittadini, ma anche promotrici di un ecosistema tecnologico dove la trasparenza, la partecipazione e la

responsabilità sono al centro della progettazione e dell'implementazione. Solo abbracciando questa visione potremo realmente sfruttare le potenzialità dell'intelligenza artificiale, navigando in modo sagace tra le complessità normative ed etiche, per costruire un mondo più giusto, equo e cosciente.

Il supporto delle istituzioni e delle autorità è fondamentale nel percorrere il cammino verso un mondo più giusto, equo e consapevole. La bozza di linee guida rappresenta un esempio tangibile di questo sostegno, dimostrando l'impegno presente e l'intenzione di costruire un futuro che rispetti tali ideali. Solo abbracciando questa visione possiamo davvero sfruttare le potenzialità dell'intelligenza artificiale, manovrando con saggezza tra le complessità normative ed etiche, al fine di edificare una società che incarni equità e consapevolezza.

Contribution of Francisco Garcia-Garrido in the framework of the procedure "Public Consultation – Bozza di linee guida per l'adozione di IA nella pubblica amministrazione". Francisco Garcia-Garrido is a Spanish lawyer, PhD in Administrative Law at the University of Trento. Partner & Legal Counsel at Himmel Advisors S.r.l. Francisco Garcia-Garrido is a member of the National Agency for Artificial Intelligence (ENIA) & European Data Protection Board (List),