Camera dei deputati
X Commissione
Indagine conoscitiva sull'intelligenza artificiale: opportunità e rischi per il sistema produttivo italiano
Memoria del Presidente del Garante per la protezione dei dati personali
Prof. Pasquale Stanzione

Ringrazio la Commissione per quest'invito, che sottende la consapevolezza della rilevanza della protezione dati nel governo dell'intelligenza artificiale (*infra*: i.a.). Essa è divenuta oggetto di dibattito politico a livello globale, in particolare dopo la diffusione dell'i.a. generativa. E questo, essenzialmente in ragione della capacità simulativa, rispetto al ragionamento umano, di questo tipo di i.a., capace di svolgere analisi di tipo semantico e quindi anche, potenzialmente, di sostituire l'uomo in determinate funzioni.. Anche per questa ragione i Ministri del digitale riuniti al G7 di Tokyo, già lo scorso anno hanno convenuto sull'opportunità di una regolazione globale dell'i.a., per renderla affidabile, "in linea con i (comuni) valori democratici condivisi". E mentre negli Usa ci si limita a un Executive Order rivolto alle Agenzie federali, l'Europa giunge all'approvazione di un regolamento generale dell'i.a., affidando a una direttiva i profili di responsabilità. Ma già nel 2016 l'UE aveva elaborato una prima disciplina dell'i.a., attraverso l'art. 22 del Regolamento (UE) 2016/679 (*infra:* Gdpr).

Se, infatti, il Garante è potuto intervenire su Chat GPT e, prima ancora, sul chatbot Replika, è perché la disciplina di protezione dati regola (e continuerà a farlo anche dopo l'AI Act) il fulcro dell'i.a.: il trattamento di dati personali funzionale a processi decisionali automatizzati e all'addestramento dell'algoritmo.

Rispetto a questo nucleo centrale dell'i.a., la disciplina di protezione dati offre alcune garanzie essenziali: il principio di conoscibilità (che esclude la legittimità di algoritmi black-box riconoscendo il diritto di ricevere informazioni significative sulla logica utilizzata), quello di non esclusività della decisione algoritmica che impone un intervento umano capace di controllare, validare o smentire la decisione automatizzata, il divieto di discriminazione algoritmica, un generale principio di trasparenza che impone precisi obblighi informativi nei confronti dell'utente, un criterio di qualità ed esattezza dei dati da utilizzare, particolarmente rilevante per evitare i bias propri di un addestramento dell'algoritmo sulla base di informazioni inesatte o non sufficientemente rappresentative. Le garanzie particolari accordate nel trattamento dei dati dei minori si sono, inoltre, rivelate determinanti nell'assicurare il doveroso controllo sull'accesso degli infraquattordicenni ad alcuni dei contenuti offerti da questi chatbot, ritenuti inadeguati (ad esempio perché sessualmente espliciti) per il loro grado di sviluppo cognitivo, etico, personologico.

I principi sanciti dalla disciplina privacy hanno, così, già assunto un valore determinante nella regolazione dei processi algoritmici, al punto da aver consentito, ad esempio alla giurisprudenza amministrativa, di rinvenirvi la disciplina di alcune determinate fattispecie e appunto, al Garante, di conformare l'utilizzo dell'i.a. con i valori propri dell'ordinamento costituzionale ed europeo. Lungi dal frenare l'innovazione, il Garante l'ha semmai promossa indirizzandola in una direzione democraticamente sostenibile e compatibile con la tutela della persona.

Questo spiega non solo perché l'AI Act si fondi anche sull'art. 16 TFUE (base giuridica della normativa in materia di protezione dati) ma, soprattutto, perché mutui, dal Gdpr, molte opzioni di politica legislativa: ad esempio la tassonomia dei divieti e delle regole applicabili, fondata sul grado di rischiosità dei sistemi, la valutazione d'impatto (qui sui diritti fondamentali) per le applicazioni ad alto rischio, il principio di trasparenza quale cardine del rapporto tra utilizzo della tecnica e autodeterminazione della persona, le garanzie rafforzate per i dati "sensibili" (recte: appartenenti a categorie particolari), il sistema dei diritti, delle tutele e delle sanzioni, la governance nella sua duplice dimensione interna e sovranazionale.

La dimensione "costituzionale" dell'AI Act (quale aspirazione alla tutela dei diritti e delle libertà fondamentali dai rischi potenzialmente derivanti da un uso anomico della tecnica) onererà, tuttavia, il legislatore interno, in fase discendente, della previsione di adeguate garanzie di indipendenza dell'Autorità nazionale competente. L'impatto, significativo e trasversale, dell'i.a. sui diritti fondamentali suggerisce, infatti, di attribuirne la competenza ad Autorità caratterizzate da requisiti d'indipendenza, in ragione dei "limiti e delle aporie" che la regola maggioritaria presenta, come insegnava Norberto Bobbio, di fronte a quel "territorio di frontiera" rappresentato dai diritti di libertà.

In ragione della stretta interrelazione tra i.a. e privacy, della competenza già acquisita in materia dalle Autorità di controllo sul processo decisionale automatizzato, che comunque andrebbe salvaguardata ai sensi degli artt. 8 CDFUE e 16 TFUE e delle caratteristiche d'indipendenza che ne connotano lo statuto, sarebbe utile ragionare sulla soluzione proposta dal Comitato europeo per la protezione dati e dal Garante europeo, volta a suggerire l'individuazione, nelle Autorità di protezione dati, delle autorità di controllo per l'i.a.

La "designazione delle autorità per la protezione dei dati come autorità nazionali di controllo assicurerebbe", infatti, come sottolineato dagli organismi europei, "un approccio normativo più armonizzato e contribuirebbe all'adozione di un'interpretazione coerente delle disposizioni in materia di trattamento dei dati nonché a evitare contraddizioni nella loro applicazione nei diversi Stati membri". Tale soluzione garantirebbe, inoltre, una notevole semplificazione per gli utenti, che dovrebbero rivolgersi a un'unica autorità per i sistemi di i.a. che operino su dati personali, una maggiore coerenza della disciplina complessivamente considerata, nonché l'estensione dello statuto di garanzie (anche in termini di indipendenza) delle Autorità di protezione dati al settore dell'i.a..

Questa scelta verrebbe incontro anche alle preoccupazioni espresse dal Governo, nella scorsa legislatura, in ordine agli oneri, amministrativi e finanziari, connessi all'attuazione dell'AI Act, nonché ai tempi eccessivamente lunghi di attuazione, imputabili alla complessità del meccanismo di governance, che "sposterebbe sulle autorità nazionali una serie di responsabilità e competenze al momento difficilmente rilevabili negli Stati membri" (come si legge nella relazione trasmessa al Parlamento in attuazione della legge n. 234 del 2012).

L'individuazione nel Garante dell'autorità di controllo per l'AI Act consentirebbe, infatti, un adeguamento quantomai tempestivo agli obblighi ivi previsti, riducendone gli oneri, potendo esso avvalersi dell'esperienza già maturata rispetto a quell'aspetto così dirimente dell'i.a. che è rappresentato dal processo decisionale automatizzato.

Le Autorità di protezione dati (e il Garante italiano, naturalmente, non di meno) possiedono, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione pienamente coerente dell'AI Act e un'applicazione lungimirante delle sue disposizioni.

Il Garante – come del resto tutte le altre Autorità di protezione dati degli Stati membri – ben potrebbe, infatti, assicurare entrambi questi obiettivi, in una prospettiva anche di riduzione degli oneri amministrativi (unificando in un'unica Autorità gli adempimenti previsti dalle due discipline) e di coerenza complessiva dell'applicazione della normativa europea in materia.

Il Garante italiano, in particolare, si è occupato dell'uso dell'i.a. negli ambiti più vari: rispetto al riconoscimento facciale a fini di polizia (sistemi Sari e Sari Real Time: cfr. rispettivamente, provv.ti 26 febbraio 2020, n. 54, doc. web n. 9309458 e 25 marzo 2021, n. 127, doc. web n. 9575877), all'ambito fiscale, in chiave di contrasto all'evasione (v. in merito, il parere del 22 dicembre 2021, n. 453, sullo schema di decreto attuativo dell'art. 1, comma 683, della legge 27 dicembre 2019, n. 160, doc. web n. 9738520, e, da ultimo, il parere dell'11 gennaio 2024, n. 3 su uno schema di decreto legislativo in materia di procedimento accertativo, adottato nell'esercizio della delega legislativa prevista dall'articolo 17 della legge 11 agosto 2023, n. 111, doc. web n. 9978230); in quello sanitario, in relazione alla cd. medicina di iniziativa (parere 16 dicembre 2021, n. 431, doc. web n. 9738538), alla riforma del Fascicolo sanitario elettronico e all'istituzione dell'Ecosistema dei dati sanitari (Eds),

nel quale si è prefigurato uno spazio per l'applicazione dell'IA (provv.ti 22 agosto 2022, nn. 294, doc. web n. 9802729 e 295, doc. web n. 9802752) e, da ultimo, con il Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale (10 ottobre 2023, doc. web n. 9938038). Particolarmente significativa, anche per l'ampia eco riscossa (anche al di fuori dei confini nazionali), l'attività di controllo svolta nei confronti di taluni operatori della cd. gig economy (provv.ti 10 giugno 2021, n. 234, doc. web n. 9675440 − oggetto di integrale conferma da parte di Corte di Cassazione, Sez. I civ., 22 settembre 2023, n. 27189 −, e del 22 luglio 2021, n. 285, doc. web n. 9685994). Vademecum sono stati dedicati al tema dei deepfake (doc. web n. 9512226) e degli assistenti digitali (doc. web n. 9696995). Tra le attività in corso di svolgimento, infine, una menzione particolare può essere fatta al procedimento nei confronti di OpenAI (in relazione a chatGPT) e l'indagine conoscitiva in materia di webscraping.

Nella cornice sovranazionale, l'Autorità partecipa anche ai lavori della G7 DPA Roundtable, che nell'anno di Presidenza italiana del G7 si concentrerà sui profili dell'IA generativa; entro la cerchia della Global privacy assembly (GPA), il Garante ha operato fattivamente nel GPA Working Group on Ethics and Data Protection in AI (AIWG), contribuendo alla predisposizione del Technical report dedicato al Risk management nel contesto dell'IA (cfr. Risks for Rights and Freedoms of Individuals Posed by Artificial Intelligence Systems - Proposal for a General Risk Management Framework, AIWG Action Point n. 6, in https://globalprivacyassembly.org) e, nel 2023, promuovendo la "Resolution on Artificial Intelligence and Employment" e la "Resolution on Generative Artificial Intelligence Systems"; segue i lavori dell'OECD e, dal 2022, ha preso parte, per il tramite di un proprio rappresentante e cooperando con il Ministero degli Esteri, ai lavori del Comitato sull'intelligenza artificiale per la redazione della Convenzione quadro sull'intelligenza artificiale del Consiglio d'Europa i cui lavori sono in fase conclusiva.

Peraltro, dal 2021 il Garante (prima fra le Autorità europee, seguita da quella francese nel 2023) ha istituito un'unità organizzativa specifica dedicata all'intelligenza artificiale, che si relaziona con alcuni tavoli di lavoro in materia di standardizzazione istituiti presso il CEN/CENELEC JTC 21 (in particolare dedicati ai profili della individuazione e gestione dei rischi connessi all'IA nonché al tema della cd. data quality) e ha stipulato nel 2022 un accordo quadro di durata triennale con il Consorzio interuniversitario nazionale per l'informatica, in particolare con i Lab nazionali dedicati all'"IA".

Non posso, conclusivamente, che suggerire alla Commissione – come già due anni fa in sede di audizione sull'AI Act- una riflessione su questo aspetto, nella consapevolezza di quanto la sinergia tra le due discipline – e, quindi, la loro applicazione da parte di un'unica Autorità- sia determinante per l'effettività dei diritti e delle garanzie che sanciscono, con significativa lungimiranza.