Potere tecnologico e strumenti di garanzia dei diritti

di Pasquale Stanzione

Con grande piacere l'Autorità ospita, oggi, questo confronto – certamente stimolante – su un aspetto di così grande rilievo, quale il rapporto dell'i.a. con la protezione dei dati.

Si discute spesso di quando datare il fenomeno della "democratizzazione" dell'i.a., ovvero della sua utilizzazione in modo trasversale ai vari settori e ai contesti sociali. Ebbene, per quanto riguarda non solo l'Europa, un anno determinante è stato proprio il 2023, con la diffusione quasi capillare dell'i.a. generativa, che a marzo scorso ha indotto addirittura mille esponenti delle big tech a suggerire, con una lettera aperta, una moratoria sullo sviluppo di questa neotecnologia, ritenuto eccessivamente rapido. Ora, al di là del merito, questo dimostra come effettivamente l'i.a. sia ormai entrata a far parte del nostro orizzonte quotidiano di vita, con effetti della cui portata (in senso lato antropologica) non siamo, forse, del tutto consapevoli. Il diritto ha il compito di colmare questo vuoto di consapevolezza, fornendoci gli strumenti per capire come porre realmente al servizio dell'uomo quella che può rappresentare tanto uno straordinario fattore di sviluppo quanto anche, se non ben governata, una fonte di rischi tutt'altro che trascurabili, per la persona, per la società, per la democrazia.

La disciplina di protezione dei dati ha introdotto dei fondamentali presidi, in questo senso, sin dal 2016.

Se, infatti, il Garante è potuto intervenire, proprio lo scorso anno, 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 dei 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,

DPCE online
ISSN: 2037-6677

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 della 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 regolazione di alcune determinate fattispecie e appunto, al Garante, di conformare l'utilizzo dell'i.a. con i valori propri dell'ordinamento costituzionale ed europeo.

Questo spiega non solo perché l'*AI Act* si fondi anche sull'art. 16 *TFUE* (base giuridica della normativa in materia di protezione dei 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.

L'*AI Act* rappresenta una pietra miliare nella regolazione delle neotecnologie: la prima disciplina al mondo, di taglio generale, dell'i.a., considerando che quella americana è un mero *Executive Order*, rivolto, come tale, alle sole agenzie federali e dal contenuto alquanto limitato. Ed è significativo che la "primazia", cronologica ma anche assiologica, nella regolazione di questa straordinaria tecnologia (dalle potenzialità preziose ma anche rischiose, se non ben regolate) spetti all'Europa. A ciascuna delle norme dell'*AI Act* è, infatti, sottesa una linea chiara di politica del diritto, che mai come nel caso della *governance* del digitale esprime i valori europei, la stessa identità dell'Unione Europea come "comunità di diritto". L'aspirazione a rendere l'i.a. "trustworthy", affidabile e la sua disciplina "future-proof" racconta molto, infatti, dell'idea europea di innovazione e, al contempo, della tutela della persona (da garantire anche rispetto a usi distorsivi della tecnica) che, secondo la Carta di Nizza , è posta al centro della stessa azione dell'Unione.

Il fulcro della normativa europea risiede nella convergenza tra innovazione e libertà, espressa in particolare dalla scelta di vietare alcuni usi dell'intelligenza artificiale, perché potenzialmente idonei a violare la dignità umana, la libertà cognitiva o amplificare le discriminazioni dalle quali, invece, proprio le macchine avrebbero dovuto liberarci. Di qui, ad esempio, il divieto di ricorso al riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, alla manipolazione comportamentale cognitiva o a tecniche tali da sfruttare le vulnerabilità soggettive o, ancora, al *social scoring*. La classificazione delle persone in base al comportamento sociale, alla condizione socio-economica, alle caratteristiche soggettive, già di per sé problematica, lo diviene ancor più - come dimostra il sistema antifrode olandese *Syri* - se affidata a un algoritmo, con *bias* che possono caratterizzarlo (per scarsa inclusività e sub-rappresentatività del *set* di dati su cui si è formato), distorcendone l'esito.

Significativi sono anche i limiti posti alla congiunzione tra potere investigativo e potenza della tecnica, che impone condizioni tanto più stringenti quanto più avanzato sia il grado d'autonomia decisionale della macchina. Così, si vietano alcuni sistemi di polizia predittiva e si circoscrivono le eccezioni al divieto di riconoscimento facciale, in luoghi pubblici.

L'utilizzo dell'intelligenza artificiale nel settore investigativo necessita, infatti, di cautele tali da scongiurare il rischio della delega, all'algoritmo, di attività potenzialmente incidenti sulla libertà personale e della sorveglianza massiva. Ciò che si teme non è tanto e non è solo il "pendio scivoloso", quanto la tendenza all'acritica accettazione sociale di una progressiva limitazione della libertà.

Per altro verso, l'utilizzo dell'i.a. nel campo della ricerca è agevolato e tanto più potrà essere valorizzato grazie alla possibilità di condivisione dei dati a fini solidaristici e, appunto, di promozione della ricerca consentita dal *Data Governance Act*, con l'innovativo istituto dell'altruismo dei dati.

Si introduce, dunque, una cornice regolatoria essenziale, ma dalla vocazione chiaramente costituzionale (in ragione della sua attitudine a sancire garanzie rispetto al potere, in questo caso tecnologico) che, lungi dal bloccare l'innovazione, l'indirizzi verso una direzione democraticamente, antropologicamente e socialmente sostenibile.

Perché, in altri termini, sia la tecnica al servizio dell'uomo e non viceversa. Come del resto è stato per il *GDPR*, che non a caso reca appunto quest'obiettivo nella parte più "programmatica" dei suoi Considerando, al quarto, assegnandogli la funzione di una dichiarazione d'intenti, di principio e di valore che è stato ed è, tuttora, il baricentro del rapporto tra innovazione, libertà, democrazia.

Pasquale Stanzione
Presidente Autorità Garante per la protezione dei dati personali
protocollo@gpdp.it

DPCE online
ISSN: 2037-6677