GIUSTIZIA INSIEME

Diritto e innovazione

Il draft di regolamento europeo sull'intelligenza artificiale

di Antonello Soro

6 maggio 2021

Il draft di regolamento europeo sull'intelligenza artificiale

di Antonello Soro*

La proposta di Regolamento europeo per l'intelligenza artificiale interviene in uno scenario di grandi cambiamenti economici, sociali, geopolitici in larga misura connessi con lo sviluppo delle tecnologie digitali.

La rapida evoluzione dei sistemi di intelligenza artificiale – come si afferma nel Considerando 1 – ottimizzando le operazioni e l'allocazione delle risorse e personalizzando la fornitura di servizi, supporta il raggiungimento di risultati vantaggiosi, sia dal punto di vista sociale che da quello ambientale, in ogni settore dell'economia.

L'assunzione di lavoratori, la determinazione dell'affidabilità per un prestito, la valutazione della capacità di un insegnante, persino il rating di legalità ai fini dell'aggiudicazione degli appalti sono sempre meno il frutto di una scelta umana e sempre più l'esito di selezioni algoritmiche, alle quali deleghiamo, quasi fideisticamente, il compito di decidere aspetti determinanti della vita delle persone.

Con l'intelligenza artificiale, la tecnica è divenuta un "fatto sociale totale", essenzialmente perché da protesica si è resa mimetica, capace cioè di replicare, fino a sostituire, gli aspetti più qualificanti dell'uomo come la razionalità, marginalizzando, in molte circostanze, il contributo

umano nel processo decisionale.

La capacità di autonomizzazione della macchina rispetto all'uomo che l'ha progettata richiama l'idea dell'automa che si emancipa dal suo creatore, evocativa di quell'ambivalenza attribuita alla macchina dal pensiero greco: tanto strumento quanto inganno.

Tra gli inganni di cui, assieme agli indiscutibili benefici, l'intelligenza artificiale può farsi portatrice vi è quello dei pregiudizi o delle inesattezze, tali da compromettere la neutralità degli stessi processi decisionali.

La delega quasi fideistica agli "oracoli digitali", dai quali ci si attende quell'obiettività che le "troppo umane" decisioni tradizionali non assicurerebbero, finisce con l'oscurarne i rischi di discriminazioni, anche etniche, che replicano in una sorta di fisiognomica computazionale pregiudizi, a volte, addirittura lombrosiani.

In questa cornice si dispiega la competizione per la leadership tra Cina e Stati uniti, rispetto alla quale l'Europa ha accumulato un ritardo non banale.

Per invertire questa tendenza, l'Unione europea ha l'ambizione di proporsi- a livello globale- come punto di riferimento per una disciplina organica della società digitale, compensando quel ritardo con posizioni di avanguardia sul piano regolatorio.

Proprio su questo punto, con il Gdpr e la direttiva 680, già nel 2016 l'Europa aveva sancito il primo limite, anzitutto valoriale, all'intelligenza artificiale, oltre il quale non si deve fare tutto ciò che è possibile fare.

Il divieto di discriminazione, unitamente al diritto alla spiegazione e alla revisione umana della decisione automatizzata, ha rappresentato (e continuerà a rappresentare, almeno fino all'approvazione delle prossime norme) il presupposto per non rendere talmente regressivo da apparire distopico, quello che invece dovrebbe rappresentare uno strumento di progresso sociale.

Questi principi essenziali sono sviluppati ulteriormente nella proposta della Commissione, che sottende una scelta importante, dal punto di vista non solo normativo ma anche e soprattutto politico, valoriale e identitario.

Esso, soprattutto se inscritto all'interno della più ampia politica del digitale portata avanti dalla Commissione assume il valore di una scelta di campo: quella di ridisegnare i confini del tecnicamente possibile alla luce di ciò che è giuridicamente ed eticamente accettabile, di temperare l'algocrazia con l'algoretica.

Significativa, in questo senso, la dichiarazione della vice-presidente Vestager, volta a sottolineare come la proposta di Regolamento coniughi l'aspirazione a una "tecnologia etica" con esigenze di sviluppo e competitività dell'Europa.

Il vantaggio competitivo cui la Commissione mira con questa disciplina è essenzialmente quello di promuovere ed esportare un modello tecnologico all'avanguardia soprattutto in termini di sicurezza ed esattezza del processo algoritmico, utilizzando dati privi di errori sistemici ai fini dell'addestramento degli algoritmi e con un costante monitoraggio della loro applicazione anche successivamente all'immissione nel mercato.

Si tratta di una previsione importante, che coglie uno degli aspetti trasformativi dell'intelligenza artificiale: il suo intrinseco dinamismo e la capacità di molti sistemi di sviluppare un apprendimento, almeno in parte autonomo, rispetto a quello progettato.

Per questo tipo di programmi, la valutazione di conformità prevista dal Regolamento dovrà essere progressiva e costante, adeguando l'analisi di impatto e compliance all'evoluzione delle nuove funzionalità "apprese" e sviluppate dal software.

Le garanzie e i limiti previsti mirano, del resto, a promuovere quella fiducia nell'innovazione evocata più volte nei considerando, senza la quale quest'ultima sarà vissuta come un processo imposto, dalla cui opacità rifuggire, anziché come una straordinaria opportunità di progresso sociale.

Si consolida così, anche in termini geopolitici, la specificità europea nell'approccio alle nuove tecnologie già emersa con il Gdpr: un'alternativa tanto al liberismo quasi anomico americano quanto al dirigismo e autoritarismo digitale cinese, fondato sull'alleanza tra potenza di calcolo e coercizione.

La stessa idea di sovranità digitale sottesa al progetto del cloud europeo, tutt'altro che un sovranismo antagonista, esprime un'esigenza di emancipazione del proprio sviluppo tecnologico dalla dipendenza costante da altri ordinamenti, fondati su scale di valori diverse che, inevitabilmente, innervano anche la tecnica, condizionandone l'uso.

Scegliendo di normare per prima una materia destinata a segnare come poche altre il futuro delle democrazie, l'Europa accosta all'idea di un'egemonia soltanto commerciale nel dominio della tecnica quella di un'egemonia valoriale, tale da imprimere al progresso una direzione antropocentrica.

Si riafferma così quella radice personalista espressa dal preambolo della Carta di Nizza con l'enunciazione della persona come centro dell'azione dell'Unione e dall'inviolabilità della dignità, la cui previsione apre il catalogo dei diritti, ritessendone la trama.

La proposta di Regolamento sottende scelte importanti.

Da un lato, infatti, rileva la scelta in favore della regolazione, che marca la distanza dall'approccio americano, ove a norme cogenti spesso si preferisce la soft law delle linee guida.

La scelta europea di introdurre un apparato normativo articolato è tanto più rilevante in un contesto, quale quello in esame, in cui la tendenza all'anomia -barattata per libertà d'iniziativa economica- finisce per relegare alla legge del mercato la definizione del perimetro di diritti e libertà, determinando non eguaglianza ma subalternità all'imperativo del profitto.

Quest'idea di fondo accomuna tutta la politica europea del digitale, a partire dal Gdpr sino alle più recenti proposte di Data Governance, Digital Services e Digital Markets Act.

E non è un caso che per tutti questi atti si sia scelta (come anche appunto per l'intelligenza artificiale) la fonte regolamentare, che si consolida sempre più come la forma tipica della disciplina europea del digitale, realizzando quella vocazione unitaria ("one continent, one law") in cui si esprimono scelte normative cui l'Europa ascrive valenza identitaria.

In questo la politica dell'Ue, dalla protezione dati all'intelligenza artificiale, passando per la disciplina delle piattaforme, sottende l'aspirazione a *fare della civiltà digitale un nuovo umanesimo*, un fattore di progresso sociale attorno a cui rivitalizzare la stessa idea della cittadinanza europea e dell'Unione come "Comunità di diritto".

Sembra, insomma, che attorno al rapporto tra uomo e macchine, diritto e tecnica, possa fondarsi un nuovo Manifesto di Ventotene, declinando in forme nuove quella dialettica tra libertà e solidarietà sociale attorno a cui si è costruito il progetto europeo.

Oggetto della disciplina sono:

- regole trasversali per l'immissione nel mercato e l'uso di sistemi di intelligenza artificiale;

- divieto del ricorso a determinati usi della stessa;

- requisiti specifici per i sistemi ad alto rischio;

- obblighi di trasparenza per forme d'intelligenza artificiale progettate per interagire con le persone, sistemi di rilevazione delle emozioni e di categorizzazione biometrica, ovvero volti a manipolare immagini o contenuti audio o video (come per il deep fake), dovendo l'utente essere

avvertito del fatto che sta relazionandosi con un robot*; e ancora*

- obblighi di monitoraggio successivi all'immissione in mercato e misure di sorveglianza.

Dai limiti di applicazione del diritto dell'Unione derivano, poi, le conseguenti (ma tutt'altro che irrilevanti) esclusioni dell'ambito applicativo del Regolamento, che interessano i sistemi d'intelligenza artificiale progettati o utilizzati esclusivamente a fini militari (esclusione espressa), è da ritenere, a soli fini di sicurezza nazionale, essendo questa materia sottratta al diritto europeo, con un'esenzione che oggi mostra però sempre più i suoi limiti.

Non si tratta, infatti, di esclusioni marginali, in quanto in questi ambiti – come ha sottolineato lo stesso Parlamento europeo nelle recenti Linee guida – l'intelligenza artificiale incontra sviluppi importanti e potenzialmente pericolosi, rispetto ai quali dunque spetta al legislatore nazionale intervenire.

Tuttavia, è da ritenere che nel caso di sistemi dual use, il Regolamento si applichi almeno al segmento di utilizzo a fini civili.

È poi rimesso a un separato atto regolamentare, ancora non presentato, lo statuto della responsabilità civile, modulato in termini di responsabilità oggettiva per i sistemi presuntivamente ritenuti ad alto rischio e di responsabilità aggravata (per colpa presunta), sul modello delineato dal Gdpr.

Dalla disciplina di protezione dati (che ha rappresentato in un certo senso l'avanguardia nella regolazione del digitale) si mutuano, del resto, altri istituti importanti:

- l'approccio fondato sul rischio con i correlativi, proporzionali adempimenti;

- gli obblighi di trasparenza verso gli utenti;

- l'articolazione del sistema sanzionatorio con cornici edittali riferite al fatturato in modo da esercitare maggiore deterrenza;

- l'ambito oggettivo di applicazione modulato sul criterio del "targeting" e dunque della localizzazione dei destinatari dell'offerta produttiva, così da determinare un'indiretta extraterritorialità della normativa;

- le certificazioni e i codici di condotta quali espressione di co-regolazione e sussidiarietà orizzontale, volti a promuovere la compliance come fattore reputazionale e dunque di vantaggio competitivo;

- l'obbligo di comunicazione degli "incidenti" suscettibili di determinare pregiudizi a terzi;

- alcune soluzioni ordinamentali quale quella della cooperazione decentralizzata tra autorità nazionali all'interno del Comitato europeo per l'intelligenza artificiale, cui partecipa anche il Garante europeo per la protezione dati.

L'architettura regolatoria si fonda su una definizione dell'intelligenza artificiale tecnologicamente neutra e su una distinzione dei relativi sistemi sulla base della loro rischiosità.

In primo luogo, si vietano i sistemi idonei a determinare discriminazioni o forme di sorveglianza inaccettabili.

I sistemi presuntivamente ritenuti ad alto rischio per caratteristiche intrinseche (o per usi in contesti cruciali quali la gestione d'infrastrutture critiche, istruzione, occupazione, servizi pubblici essenziali, controllo delle frontiere, amministrazione della giustizia, attività di contrasto) sono assoggettati a un articolato apparato di vincoli e cautele ex ante ed ex post che responsabilizza, in misura proporzionale, i vari soggetti coinvolti nella filiera produttiva (un efficace sistema di gestione del rischio, oneri probatori funzionali al principio di responsabilizzazione, valutazione di conformità modulata su standard di riferimento e certificazioni, garanzie di supervisione umana).

Vi sono poi i sistemi d'intelligenza artificiale soggetti ad obblighi di trasparenza peculiari in ragione della loro incidenza sulla persona e, soprattutto, sul processo motivazionale e cognitivo.

Infine, i sistemi a rischio basso o minimo, sono sottratti al reticolato di vincoli più puntuali su descritto in ragione della sostanziale irrilevanza del pericolo stimato nel loro uso.

Rileva anche, quale misura di promozione dell'innovazione, la disciplina di sandboxes regolamentari, volte a consentire lo sviluppo di servizi d'intelligenza artificiale con la supervisione delle autorità competenti, così da favorire la conformità normativa di soluzioni in certa misura sperimentali.

Particolarmente rilevanti sono i divieti, che concorrono a definire il limite esterno dell'intelligenza artificiale eticamente e socialmente sostenibile, riaffermando l'intangibilità dei diritti fondamentali, dell'eguaglianza e della dignità rispetto alle nuove subalternità indotte dalla tecnica.

Si vieta quindi il ricorso a sistemi che sviluppino tecniche subliminali idonee a condizionare il comportamento altrui o che sfruttino le vulnerabilità di gruppi sociali, nonché a sistemi di social scoring fondati sul monitoraggio delle condotte individuali.

Si tratta di una previsione rilevante in termini valoriali e che non soltanto marca la differenza del modello europeo rispetto a quello cinese, ma che ammonisce anche rispetto a quelle tendenze, presenti in molti Paesi dell'Unione, a utilizzare, per l'erogazione di prestazioni di welfare e il controllo sulla legittimità della loro assegnazione, algoritmi suscettibili di determinare una profilazione su base censitaria della popolazione, dagli effetti potenzialmente discriminatori.

In Olanda – ad esempio – si è utilizzato un sistema di verifica antifrode (SyRI) ritenuto illegittimo dalle corti interne e definito strumento al servizio dello "Stato di sorveglianza per i poveri" dall'alto rappresentante Onu per i diritti umani, in quanto idoneo a colpire, con un monitoraggio socialmente selettivo, proprio le frange deboli della popolazione.

Particolare rilievo assume poi, nella proposta, il divieto di ricorso per finalità di contrasto a sistemi d'identificazione biometrica, in tempo reale, salva l'indispensabilità per esigenze pubblicistiche imperative.

Questo criterio di residualità, conforme peraltro alla posizione espressa dal Consiglio d'Europa, ha orientato la decisione del Garante nel parere negativo sul sistema Sari real time e, per altro verso, la recente pdl Sensi sulla moratoria dell'uso di tali tecniche.

È auspicabile che questa facoltà venga esercitata con assoluto rigore, pena una sostanziale elusione del divieto di ricorso a sistemi d'intelligenza artificiale, il cui rischio è ritenuto inaccettabile per il sistema di valori proprio dell'ordinamento europeo.

Le deroghe al divieto, previste dal testo del regolamento, devono infatti essere intese conformemente a quel bilanciamento tra libertà e sicurezza attorno a cui la giurisprudenza della Cgue ha affermato la centralità della privacy per l'identità costituzionale europea.

Soltanto nell'ultimo anno, con tre pronunce (Schrems II, Privacy international e quella del 2 marzo sulla data retention) la Corte ha fatto delle garanzie accordate alla privacy rispetto alle esigenze investigative il fulcro del rapporto tra libertà e sicurezza, declinandolo non in chiave antagonista ma sinergica, secondo quel binomio sancito dall'art. 6 della Carta di Nizza.

Ecco, dunque, che sul terreno dell'intelligenza artificiale e della sua regolazione si gioca una partita cruciale per il futuro dello Stato di diritto in ogni suo aspetto, per impedire che la tecnologia, con un'eterogenesi dei fini, divenga il nuovo Leviatano da cui il processo democratico aveva affrancato il cittadino.

La democrazia può dirsi ancora tale finché siamo noi a creare gli algoritmi e non gli algoritmi a creare noi, anticipando e indirizzando desideri, esigenze, paure.

Fin quando, dunque, la tecnica resti ancora al servizio dell’uomo, essa potrà dirsi alleata e non antagonista della democrazia.

Il Regolamento sull’intelligenza artificiale può essere davvero un passo molto importante nella direzione del “principio di responsabilità” (più ampio della sola idea di responsabilizzazione) che deve ispirare il rapporto tra uomo e tecnica.

Il percorso è ancora lungo e l’esito non è scontato, ma abbiamo il dovere di essere ottimisti.

***già Presidente del Garante per la protezione dei dati personali**