AI Act e *digital constitutionalism*

Andrea Simoncini
Professore ordinario di Diritto Costituzionale, Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze. Mail: andrea.simoncini@unifi.it

L'AI Act può essere considerato una componente del *digital constitutionalism*?
Una domanda del genere, se vogliamo evitare l'abitudine invalsa ormai anche tra gli studiosi di "tifare" per fazioni opposte, non può che essere articolata.
La nuova normativa europea saprà davvero offrire strumenti adeguati per limitare e disciplinare il crescente potere persuasivo delle tecnologie decisionali?
Innanzitutto, essendo ancora in fase di attuazione, il giudizio non potrà che essere prospettico e prognostico. Moltissimo dipenderà dalla attuazione che effettivamente verrà data a questo nuovo regolamento. In ogni caso, però, comunque lo si consideri, l'AI Act rappresenta un intervento normativo di vastissima portata, certamente in grado di avere un impatto rilevante sul grado di protezione e godimento delle libertà fondamentali nello spazio europeo e, per questo, un elemento di quello che considero l'ordine costituzionale europeo - comunque lo si aggettivi.
L'AI Act rappresenta, infatti, una svolta epocale nella regolazione tecnologica e un passo decisivo per il futuro dell'Europa. L'UE ha scelto di disciplinare uniformemente l'IA, mentre Stati Uniti e Cina hanno adottato strategie opposte: deregolamentazione quasi totale negli USA, rigido controllo statale in Cina.
Molto spesso si ironizza sul fatto che mentre Cina ed America producano tecnologia l'Europa si limiti a regolarla, è però un dato di fatto che l'Europa ha scelto un suo *Sonderweg*, assumendosi il rischio di tentare una strada diversa e contando sul fatto, ricordiamolo, che essa pur sempre rappresenta il mercato mondiale più ricco per i dispositivi e i servizi tecnologici.
Il regolamento cerca, come tutto il diritto europeo, un delicato e difficile equilibrio tra promozione del mercato e tutela dei diritti. Da un lato, mira a recuperare il ritardo competitivo europeo (ricordiamo che l'AI Act rimane fondato sull'art. 114 TFUE); dall'altro, si pone come scopo la protezione della salute, la sicurezza e i diritti fondamentali.
Andrà quindi chiarito in apertura: l'AI act è un regolamento che non ha come scopo *esclusivo* la protezione dei diritti, la sua natura è esplicitamente e consapevolmente compromissoria e questo carattere emerge chiaramente: non nasce come strumento orientato alla tutela dei diritti, ma come normativa industriale e di mercato che mira a garantire la sicurezza dei prodotti tecnologici. Non è uno strumento *right-based*, ma *risk-based*.
A me pare quindi che un giudizio realistico non possa che articolarsi in luci e ombre.
A. Le "luci" del regolamento
Come ho detto, il compromesso tra promozione e tutela si traduce in una regolazione *risk-based*, simile a quella dei prodotti industriali: sistemi vietati, sistemi ad alto rischio e a basso rischio. Questo approccio, pensato per l'Europa, finisce per avere un impatto globale grazie al cosiddetto "effetto Bruxelles": chi vuole operare nel mercato europeo deve rispettarne gli standard, ovunque abbia sede legale.
Tra i punti di forza principali dell'AI act vanno inseriti alcuni principi giuridici certamente di natura sostanzialmente "costituzionale". Innanzitutto, il principio che altrove ho definito di "lealtà digitale", ovverosia l'obbligo di trasparenza nelle interazioni uomo-macchina, cruciale per contrastare fenomeni come i deepfake e preservare la consapevolezza degli utenti. Il principio di "inclusività": inteso come obbligo di "sorveglianza

umana" sui sistemi ad alto rischio (art. 14); versione indubbiamente più debole del diritto a non essere soggetti a decisioni totalmente automatizzate posto dall'art. 22 del GDPR. Resta, a mio avviso, la lacuna tra le AI vietate - dovuta alla rapidità dell'evoluzione tecnologica - della cosiddetta AGI, o Intelligenza Artificiale Generale, intesa come sistemi di IA capaci di comprendere, apprendere e svolgere qualsiasi compito intellettuale che un essere umano possa svolgere, dunque, miranti esclusivamente alla sostituzione dell'essere umano. Nei confronti di questa cd. "*agentic*" AI, c'è un crescente consenso globale sul suo divieto o, quantomeno, su una moratoria nello sviluppo, vista l'assenza di sistemi efficaci di controllo e limitazione. L'AI Act pone anche un principio di "comprensibilità": inteso come obbligo di trasparenza funzionale (art. 13), che permetta agli utenti di comprendere e controllare i sistemi; anche in questo caso, è una versione ridotta rispetto al diritto generale a spiegazioni comprensibili che altrove abbiamo sostenuto. Uno dei principi in assoluto più importanti e potenzialmente rivoluzionari riguarda la "*qualità dei dati*". È posto dall'art. 10 e richiede che per l'addestramento degli algoritmi di AI nei settori ad alto rischio, vengano impiegati solo dataset rappresentativi, affidabili e privi di *bias*. Qui il Regolamento, correttamente, sposta l'attenzione dagli algoritmi ai dati usati per il *machine learning*, riconoscendone il ruolo determinante per ottenere esiti affidabili. Come sappiamo, molti sono gli interrogativi – sollevati soprattutto in ambito industriale - sulla concreta applicabilità di criteri come "completezza" o "assenza di errori" nei dataset. Altra componente fondamentale di *digital constitutionalism* è la Valutazione d'impatto sui diritti fondamentali (la c.d. FRIA). Viene posto l'obbligo per enti pubblici e privati che forniscono servizi pubblici di valutare i rischi sui diritti prima di usare IA ad alto rischio. Anche questo è uno strumento potenzialmente efficace, ma si teme che sia piuttosto oneroso per PMI e difficile da uniformare a livello europeo.

Infine, una delle novità più interessanti poste dall'AI Act è il tema delle "Regulatory sandboxes": gli spazi di sperimentazione normativa (art. 57) che consentono la possibilità di testare la conformità dei prodotti rispetto alle previsioni della regolazione in ambienti controllati ed indipendenti in cui partecipano anche i regolatori, da attivare obbligatoriamente entro il 2026. Le *Sandbox* sono considerate strumenti chiave anche dal Rapporto Draghi, poiché mirano a coniugare tutela e competitività, evitando che la regolazione freni l'innovazione e semplificando la conformità al nuovo quadro normativo.

B. Le "ombre" e le criticità

Accanto alle luci, emergono alcune criticità e mi pare che siano tre gli elementi di complessità più difficili da affrontare.

a) *Complessità interpretativa e istituzionale.* L'AI Act è un atto normativo molto rilevante (sviluppa 144 pagine sulla Gazzetta Ufficiale dell'Unione Europea) ed interagisce con molte altre normative altrettanto rilevanti (DSA, DMA, GDPR, Data Act, NIS2, CRA, DGA). La stratificazione regolatoria rischia di generare sovrapposizioni, confusioni e conflitti normativi. In Italia, ad esempio, la proposta di affidare l'attuazione dell'AI Act a due agenzie governative (ACN e AGID) suscita molte perplessità sul piano organizzativo, oltre che sostanziali, data la mancanza di indipendenza prevista dall'art. 70 dell'AI Act. La fase di interpretazione ed attuazione, inoltre, è affidata ad un vasto numero di istituzioni nazionali ed europee: autorità di settore, comitati, Commissione UE. *Ictu oculi*, stiamo parlando di centinaia di istituzioni coinvolte, con un elevato rischio di inefficienze e di conflitti di competenza positivi o negativi.

b) *Complessità politica.* L'ampiezza della portata del regolamento ha richiesto numerosi compromessi sul piano politico che hanno prodotto in alcuni casi disposizioni volutamente vaghe, rinviando spesso le scelte concrete a futuri atti tecnici. Ciò genera incertezza e lascia spazio a pressioni lobbistiche e divergenze ideologiche sul futuro sviluppo industriale del settore. Come abbiamo già detto, l'AI Act è indubbiamente un intervento normativo coraggioso, che per la prima volta disciplina un tema vastissimo con una regolazione dettagliata. Occorre, però, essere realisti e riconoscere che in molti casi una regolazione espansiva non sempre è segno di chiarezza e univocità nelle scelte normative. Ad esempio, l'AI Act, pur essendo un regolamento – fonte immediatamente applicabile - per moltissime materie chiave rinvia concretamente non solo alla legislazione attuativa degli stati nazionali di cui abbiamo già parlato, ma anche alla stessa legislazione delegata ed alla normazione tecnica europea ovvero alla regolazione da parte degli organismi di standardizzazione tecnica (ENI, UNI, ISO). Questi rinvii – come anche la tecnica di inserire parti importanti della disciplina in allegati al Regolamento – da un lato intendono dare flessibilità e possibilità di aggiornamento più rapido alle prescrizioni, ma in altri casi possono esprimere ciò che Schmitt definiva *compromesso dilatorio*; ovverosia, norme approvate con un contenuto intenzionalmente non auto-applicativo, proprio perché non si riesce a raggiungere un reale accordo a livello politico e si preferisce spostare ad una successiva sede "tecnica" la definizione concreta della regola.

c) *Ipertrofia normativa*.

Questa complessità della attuazione dell'AI act ha prodotto una reazione di scarso entusiasmo da parte del mondo industriale chiamato ad applicare le norme, sentimento che ha trovato una voce molto autorevole nel già citato rapporto Draghi sulla Competitività europea in cui si invoca a chiare lettere una forte semplificazione del quadro normativo per incentivare la capacità produttiva e concorrenziale delle aziende europee in materia di tecnologia. Draghi afferma molto nettamente che "sebbene i confronti diretti siano oscurati dai diversi sistemi politici e giuridici, negli Stati Uniti sono stati promulgati circa 3.500 testi di legge e sono state approvate circa 2.000 risoluzioni a livello federale nel corso degli ultimi tre mandati del Congresso (2019-2024). Nello stesso periodo l'UE ha approvato circa 13.000 norme. Nonostante questo crescente flusso normativo, l'UE non dispone di un quadro quantitativo per analizzare i costi e i benefici delle nuove norme".

Paradossalmente, quindi, la sfida principale, se si vuole confermare l'opzione europea per la tutela dei diritti fondamentali *attraverso* la legislazione sulla produzione tecnologica, è nell'agevolare la *compliance* con tale legislazione, semplificandola e rendendola meno onerosa. Se non accadrà tale semplificazione, il rischio principale è che tale costo della regolazione sarà considerato eccessivo – o fuori mercato - ed allora le aziende cercheranno di eluderlo o di aggirarlo, se non sceglieranno, più drasticamente altri mercati di destinazione ovvero altre sedi di stabilimento.

Questa esigenza di semplificazione interna, deve oggi misurarsi con la nuova situazione geopolitica esterna. Mi riferisco alla politica a dir poco "aggressiva" della nuova amministrazione Trump in materia di oneri e tariffe imposte sulle aziende statunitensi. Non è facile prevedere quanto i primi segnali protezionistici provenienti dalla amministrazione americana siano reali mutamenti strategici di lungo periodo ovvero solo *exploits* contingenti di natura tattica, preordinati alla rinegoziazione dei diversi accordi commerciali; comunque in atti ufficiali della Casa Bianca la regolazione europea è stata considerata una

sorta di tariffa indiretta o un onere improprio ed in quanto tale, bollata come *estorsione* (*extortion*) e per questo è considerata una delle ragioni della improvvisa scelta di introdurre dazi sulle importazioni europee. È fondamentale, dunque, una ragionevole semplificazione del quadro regolatorio, sia nell'implementazione dell'AI Act che, più in generale, nel complesso dell'emergente Digital Acquis nel diritto europeo. Questa razionalizzazione della fase attuativa è essenziale per garantire l'obiettivo principale di tali regolamenti: coniugare la crescita economica con una adeguata protezione dei diritti fondamentali. In questa prospettiva, la semplificazione deve essere vista come uno strumento per rafforzare la tutela dei diritti, e non come un tentativo di deregolamentare il settore, come potrebbe essere inteso oltreoceano.