GdP
GRUPPO di PISA
Dibattito aperto sul Diritto e la Giustizia Costituzionale

IL FORUM

IL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE *

Introduzione al *Forum*

MICHELA TROISI

Questo *forum* intende esplorare le potenzialità e i limiti del nuovo Regolamento europeo sull'intelligenza artificiale (Regolamento Ue 2024/1689), primo atto con il quale, a livello internazionale, si è proceduto ad una regolamentazione organica della materia, con l'ambizioso obiettivo di promuovere la diffusione di una intelligenza artificiale antropocentrica e affidabile. Il suddetto Regolamento procede, preliminarmente, a una definizione della nozione stessa di intelligenza artificiale o, meglio, dei sistemi di intelligenza artificiale: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» (art. 3, par. 1). La nuova disciplina impone una serie di obblighi rivolti ai fornitori e ai distributori di tecnologie di intelligenza artificiale e ne regolamenta l'autorizzazione nel mercato unico dell'Unione europea.

Le domande poste in questo *forum*, a cui partecipano alcuni tra i più profondi conoscitori della materia, si propongono di indagare profili di metodo e di merito della nuova disciplina, non tralasciando di porre all'attenzione degli interlocutori coinvolti il tema della collocazione del nuovo sistema di regolazione nel contesto nazionale.

Gli intervistati sono, innanzitutto, invitati a riflette sulle potenzialità di un atto normativo di natura regolamentare, che, direttamente e uniformemente applicabile su tutto il territorio dell'Unione, non necessita di recepimento da parte dei legislatori nazionali. Ci si sofferma, poi, sul *risk based approach*, in base al quale obblighi e

* Contributi sottoposti a referaggio ai sensi dell'art. 5 del Regolamento della Rivista.

doveri vengono graduati e adattati rispetto al rischio concreto connesso alle attività poste in essere, quale modalità di regolazione della materia e, in particolare, sulla correlazione in ipotesi sussistente tra l'utilizzo di questo approccio e le esigenze del "costituzionalismo digitale". Occorre ricordare, infatti, che il nuovo Regolamento, con una prospettiva tendenzialmente "top-down", opta per una classificazione dei sistemi di intelligenza artificiale articolata in quattro categorie, raffigurate dalla Commissione europea con una piramide: "rischio inaccettabile", "rischio elevato", "rischio limitato" e "rischio minimo". Dopo l'invito alla valorizzazione degli aspetti di maggiore interesse introdotti dalla nuova disciplina, le questioni sottoposte all'attenzione dei nostri interlocutori concernono il contesto nazionale e, in particolare, la copiosa giurisprudenza amministrativa in tema di decisone automatizzata e, in una prospettiva *de iure condendo*, la proposta di legge A.S. 1146 (XIX legislatura) recante "Disposizioni e delega al Governo in materia di intelligenza artificiale". Questa iniziativa, dai contorni chiaroscuri, ha quantomeno il merito di collocare l'Italia tra i Paesi che per primi hanno deciso di normare la materia, negli spazi che l'Europa ha lasciato ai legislatori nazionali. I mutamenti socio-tecnologici a cui stiamo assistendo, infatti, non consentono che rispetto al tema si possa rimanere indifferenti.

Siamo, dunque, particolarmente felici che la nostra Rivista possa ospitare un dibattito ricco e informato su un tema di così stringente attualità.

INDICE

I Domanda (p. 201 ss.) - Per una lunga fase, la disciplina europea in tema di intelligenza artificiale è stata affidata a strumenti di *soft law* (es. *White paper of artificial intelligence*). Ritiene che il ricorso allo strumento del regolamento sia da accogliere con favore? Quali sono le potenzialità e i limiti del ricorso a questa fonte?

II Domanda (p. 211 ss.) - L'approccio regolatorio basato sul rischio (*risk based approach*) ricorre in tutti gli ultimi regolamenti dell'Unione europea in tema di innovazione digitale. Ritiene che tale approccio risponda alle esigenze del "costituzionalismo digitale"?

III Domanda (p. 220 ss.) - Quali sono, a suo avviso, le novità di maggiore rilievo introdotte dal regolamento?

IV Domanda (p. 226 ss.) - Tra i settori ad alto rischio previsti dall'allegato 3 del regolamento, quali potranno trarre i maggiori benefici dall'utilizzo dell'intelligenza artificiale?

V Domanda (p. 234 ss.) - Guardando al contesto nazionale, ritiene che la nuova disciplina si ponga in continuità con la giurisprudenza amministrativa in tema di decisione automatizzata?

VI Domanda (p. 239 ss.) - In una prospettiva de iure condendo, come valuta la proposta di legge A.S. 1146 (XIX legislatura) "Disposizioni e delega al Governo in materia di intelligenza artificiale"?

I partecipanti al Forum (p. 252)

I Domanda

Per una lunga fase, la disciplina europea in tema di intelligenza artificiale è stata affidata a strumenti di *soft law* (es. *White paper of artificial intelligence*). Ritiene che il ricorso allo strumento del regolamento sia da accogliere con favore? Quali sono le potenzialità e i limiti del ricorso a questa fonte?

FRANCESCA BAILO

Per valutare le potenzialità e i limiti della scelta adottata dall'Unione europea di ricorrere, innanzitutto, ad una regolamentazione dei sistemi di intelligenza artificiale e, in secondo luogo, di volerlo fare attraverso uno strumento legislativo, il regolamento, che, oltre ad avere una portata generale e ad essere uniformemente e direttamente applicabile su tutto il territorio unionale, non necessita di un recepimento interno da parte dei legislatori nazionali, pare opportuno inquadrare meglio come la ridetta fonte debba essere collocata sia rispetto alle altre fonti legislative volte a dare attuazione all'Agenda Digitale Europea, sia rispetto agli atti di *soft-law* che hanno gettato le fondamenta per predisporre una tale regolamentazione.

Quanto al primo versante, il Regolamento n. 1689/2024 del 13 giugno 2024 (d'ora in poi, "*Ai Act*"), infatti, può essere considerato come una tessera fondamentale di un più ampio mosaico di atti legislativi – che comprendono il *Digital Service Act* (DSA), sui servizi digitali, il *Digital Market Act* (DMA), sui mercati digitali, e il *Data Governance Act* (DGA), in materia di *data sharing* – che, seguendo il modello regolatorio del GDPR, si pongono il comune e ambizioso obiettivo di favorire lo sviluppo del mercato unico digitale, in modo da rendere l'Unione europea maggiormente competitiva all'interno di uno scenario internazionale in cui si sono fino a questo momento fronteggiate due opposte potenze e, cioè, quella statunitense e quella cinese e, in ultimo, promuovere l'approccio europeo alla *governance* tecnologica sulla scena mondiale.

Quanto al secondo versante, l'*Ai Act* può ritenersi il punto di arrivo di una numerosa serie di atti di impulso che, almeno a far data dal 2017 (anche se non mancano alcuni veri e propri atti "precursori" che risalgono addirittura al 1985: v., ad es., la Decisione del Consiglio del 26 novembre 1985 relativa alla conclusione di un accordo Comunità-COST su un'azione concertata nel campo dell'intelligenza artificiale e del riconoscimento delle forme) hanno definito le priorità del legislatore europeo (v. già la Dichiarazione comune sulle priorità legislative per il periodo 2018-2019 (2017/C 446/01), ricomprendendo tra queste, per l'appunto, quella di garantire "un elevato livello di protezione dei dati, dei diritti digitali e delle norme etiche, pur cogliendo i benefici ed evitando i rischi degli sviluppi in materia di intelligenza artificiale e di robotica". E, del resto, il rispetto di principi etici nell'impiego dell'AI e, parimenti, l'esigenza di garantire e favorire una certa fiducia e affidabilità della stessa nel mercato, laddove i sistemi non siano giudicati a rischio "inaccettabile", sono stati veri e propri

"fari" che hanno guidato la stesura del ridetto regolamento e che trovano le basi negli atti di *soft-law* nei medesimi anni (v., ad es., la Comunicazione della Commissione europea del 2018 su "*L'intelligenza artificiale per l'Europa*" e quella del 2019 su "*Creare fiducia nell'Intelligenza Artificiale antropocentrica*"; le risoluzioni del Parlamento europeo, adottate nel 2020 e poi ampliate nel 2021, tra gli alti, sui principi etici dell'Intelligenza Artificiale, della robotica e delle tecnologie correlate, oltreché sul regime di responsabilità civile per l'AI; il Libro Bianco "*Un approccio europeo all'eccellenza e alla fiducia*" del febbraio 2020).

È in questo contesto, dunque, che può meglio comprendersi come sia maturata la scelta del legislatore eurounitario di voler per prima dettare una disciplina in materia di AI – specie rispetto alle citate due principali potenze con cui deve confrontarsi, quella americana e quella cinese – dovendosi quest'ultima verosimilmente ricondurre a obbiettivi strategici di più ampio respiro, quali l'individuazione di uno *standard*, come già fatto dal regolamento generale sulla protezione dei dati, idoneo a promuovere l'approccio europeo alla *governance* tecnologica sulla scena mondiale e, in prospettiva, l'affermarsi dell'UE quale *leader* nella regolazione della materia e la massimizzazione degli investimenti sullo sviluppo dell'AI, onde competere con le ingenti risorse finanziarie al proposito allocate sia in USA, sia in Cina.

Al di là di questi obbiettivi di natura sostanzialmente geopolitica, alla base del recente intervento normativo unionale vi è poi la ben avvertita necessità di armonizzare la disciplina in materia di AI, fissando un assetto normativo omogeneo sui principali profili giuridici che emergono dall'impiego di detta nuova tecnologia, in modo da superare e/o prevenire l'eventualità di una eccessiva eterogeneità nella regolamentazione della stessa da parte degli Stati membri, che potrebbero al contrario agire in ordine sparso specie in relazione al livello di tutela dei diritti da garantire.

Al contempo, in taluni punti, il testo del regolamento sconta un alto tasso di tecnicismo che potrebbe rappresentare un limite alla necessità di stare al passo con la rapida evoluzione a cui siffatte nuove tecnologie sono soggette, rendendo talora obsolescenti discipline appena entrate in vigore. Tuttavia, questo aspetto, che potrebbe rappresentare un vero e proprio limite, può ritenersi almeno in parte temperato per il fatto che sono contemplati anche meccanismi "flessibili" (essenzialmente mediante l'emanazione di atti delegati ai sensi dell'art 290 TFUE da parte della Commissione), in grado di consentire un continuo aggiornamento del dato normativo e tenersi così in linea di continuità con l'evoluzione tecnologica. In alcuni casi, poi, si impiega, al contrario, "clausole generali" che, talora, potrebbero dare l'idea di essere delle vere e proprie "direttive mascherate" tali da lasciare un (forse troppo?) ampio margine di manovra per gli Stati membri.

GIOVANNA DE MINICO

Il Regolamento sull'intelligenza artificiale (n. 1689/2024, da ora *AI Act*) rappresenta l'esito di un percorso legislativo lungo e complesso, anticipato da

documenti di *soft law* europeo. La COM(2018) 237 final, 25 aprile 2018, *L'intelligenza artificiale per l'Europa*; gli *Orientamenti etici per un'IA affidabile,* 8 aprile 2019 del Gruppo di esperti; e, infine, la COM(2020) 65 final, 19 febbraio 2020, *Libro bianco sull'intelligenza artificiale*. Questi Atti più che riconoscere diritti e assegnare doveri hanno indicato metodo e obiettivi alla futura *regulation*: fiducia, approccio basato sul rischio, innovazione e valori europei comuni. Nelle domande 2, 4 e 5 entrerò nel merito del Regolamento, qui invece esaminerò le fonti che avrebbero creato *ius novi* in linea con quel metodo e in risposta a quegli obiettivi. Pertanto, indicherò tre argomenti favorevoli allo strumento regolamentare, senza omettere i suoi chiaroscuri dovuti all'apertura a fonti ulteriori del diritto europee ammesse. Quanto invece agli aspetti negativi di un'auto-regolazione dominata dagli egoismi privatistici, rinvio a quanto dirò nel rispondere alla domanda n. 2.

La prima ragione a favore.

Il mio discorso è stato preceduto dalle accese discussioni del secolo scorso intorno a come disciplinare Internet; l'alternativa era secca: o si enfatizzava la Rete nella sua aspirazione anarchica come l'*heaven of the self regulation* o le si imponeva una camicia di forza regolatoria. Questa *querelle* dall'esito incompiuto ha avuto il merito di mettere in tensione gli attributi della sovranità statale: Autorità, Territorialità e Imperatività. Sul punto riprendo l'insuperabile lezione di Lessig, che nel combinare e intrecciare quattro strumenti è riuscito a disegnare una regolazione *well suited* al mezzo tecnologico (L. LESSIG, *Code Version 2.0*, New York, 2006). Ma il susseguirsi di *law, self-regulation, market and architecture* sostituisce all'iniziale domanda un'altra: esiste un ordine tra questi strumenti da osservare?

L'imposizione eteronoma delle finalità all'autoregolazione si concilia perfettamente con il principio di gerarchia delle fonti, secondo il quale il "diritto dei privati" è ammesso a integrare, completare il discorso avviato a livello primario, ma non già a iniziarlo *ex novo*, altrimenti la sua secondarietà alla legge sarebbe solo potenziale, tema al quale dedicai un'ampia parte di un mio lavoro monografico, *Regole. Comando e Consenso*, Torino, 2004, cap. II.

Sintetizzo in un'espressione la lezione fondamentale della Legge sull'IA: l'autoregolazione, se lasciata a se stessa, rimette il conseguimento del *common good* all'improbabile coincidenza con le finalità dei "governi privati di interesse", prendendo a prestito la felice espressione di A.W. STREECK – P.C. SCHMITTER, *Community Market State and Association*, in A.W. STREECK – P.C. SCHMITTER (eds.), *Private Interest Government: Beyond Market and State*, London, 1985. Nel caso in cui questa coincidenza degli interessi corporativi con il *common good* non si dovesse verificare, il secondo bene sarà sacrificato a vantaggio della tensione lucrativa.

Un'ulteriore ragione impone la priorità e la preferenza del diritto *binding* sul quello dolce: la gerarchia dei valori e il vincolo di sussidiarietà tra le fonti sono il terreno comune a ogni segmento del diritto, quindi anche alla realtà di Internet e al suo più evoluto esito tecnologico: l'intelligenza artificiale. Questa, infatti, una volta attratta alla legalità sovranazionale, deve obbedire a un bagaglio di valori a-territoriali,

quantomeno al binomio uguaglianza sostanziale/diritti fondamentali, che orizzontalmente attraversano gli ambiti virtuali più disparati dall'economia digitale alla confusa socialità delle piattaforme. L'imposizione eteronoma, salvo poi capire in che misura essa conformi il *soft law*, assolverebbe a una prestazione di risultato? Intendo dire la cornice vincolante è in grado di assicurare che il progresso tecnologico sia un'occasione di crescita per tutti, e non solo per chi da cittadino o da operatore già goda di una posizione dominate nella competizione economica o nella partecipazione democratica? Perché se così non fosse, il progresso avrà giovato solo a pochi, dando un'interpretazione *contra Constitutionem* dell'uguaglianza sostanziale (G. DE MINICO, *Diritti Regole Internet*, in *Costituzionalismo.it*, n. 2/2011), che sarebbe stata rovesciata perché la tecnica avrebbe continuato a dare a chi già aveva.

Il Regolamento sull'IA ha però solo sfiorato l'antica *issue* dell'obbedienza del *soft-law* al *common good*, e l'ha assicurata disegnando il rapporto tra eteronomia e *soft-law* in termini di subordinazione del diritto dolce alla prima nel regolare i sistemi di ultima generazione, come l'intelligenza generativa (come Chat GPT) e quelle a basso rischio. Per entrambe, infatti, sono previsti i codici di pratiche e di condotta, che implementeranno le norme fissate dal legislatore europeo [G. DE MINICO, *Internet e le sue regole*, in M. CALAMO SPECCHIA (a cura di), *Processi politici e nuove tecnologie*, Torino, 2024]. Ma la regia della Commissione saprà in grado di garantire una leale cooperazione tra il soggetto pubblico e la collettività diffusa nel *rule-making* dei codici? La prevalenza degli interessi lobbistici, già emersa in sede di triloghi dell'*AI Act,* non mi permette di riporre un'assoluta fiducia nell'autoregolazione, a meno che questa non sia guidata puntualmente dalla mano pubblica e ricondotta entro una cornice eteronoma.

2) *La scelta Regolamento in luogo della Direttiva*.

Per evitare possibili ricadute negative sulla libera circolazione dei beni, causate da normative nazionali disomogenee, la Commissione ha preferito la struttura di un atto già direttamente applicabile, che non esigesse alcuna intermediazione da parte del legislatore statale. Il Regolamento supera i difetti manifestatisi nel settore delle telecomunicazioni, dove i vari Pacchetti direttive avevano polverizzato l'unicità del mercato comune in tante piazze rionali quanti erano gli Stati membri, che agivano in una situazione di supposta anarchia normativa, lì dove le Direttive esistevano ma rimanevano inosservate nella funzione orientatrice del decisore politico interno. Il *considerandum* 3, infatti, esibisce come base legislativa l'art. 114 TFUE, norma che intende evitare le divergenze regolatorie che ostacolano la libera circolazione, l'innovazione, la diffusione dei sistemi di IA e dei suoi prodotti, stabilendo obblighi uniformi per gli operatori al fine di assicurare la tutela dei diritti fondamentali in termini omogenei sull'intero mercato interno. La previsione di strumenti di diritto dolce compensa la rigidità del Regolamento, che da fonte antica mostra la sua modernità stando al passo con l'evoluzione tecnologica. Tra questi *remedies* meritano di essere ricordati: la delega di poteri alla Commissione per modificare l'elenco delle IA vietate; la lista dell'Allegato III con i settori ad alto rischio; l'aggiornamento dei parametri di calcolo che individuano le IA a rischio sistemico; le richieste di modifiche del

regolamento e della struttura della *governance* [K. ZENNER, *The AI Act: responsibilities of the European Commission (AI Office)*, online al link: https://www.kaizenner.eu], rimane che ciascuno i questi strumenti presenta pro e contro che richiederebbero una trattazione a se stante, che sto sviluppando in un altro lavoro.

3) La terza ragione a favore del Regolamento.

Questa non è che la conseguenza diretta della seconda, appena esposta. La Commissione ha voluto sintetizzare il mercato digitale in un'unica piazza, lo dimostrano i due Regolamenti che hanno preceduto l'*AI Act*: il *Digital Markets Act* (n. 2022/1925) e il *Digital Services Act* (n. 2022/2065). In altri termini, la presenza di un ecosistema digitale, la convergenza tecnologica, il livello transfrontaliero delle IA e l'integrazione delle piattaforme e degli imprenditori digitali, compongono i tasselli di una cinghia di trasmissione, che protegge senza soluzione di continuità dall'operatore, collocato al vertice della piramide, fino all'utente finale, che si muove alla base della stessa figura geometrica.

COSTANZA NARDOCCI

Il fenomeno dell'intelligenza artificiale e i suoi rapporti con il diritto hanno attraversato fasi diverse e temporalmente diversificate.

Dall'iniziale approccio incline alla c.d. *self-regulation* dei sistemi di intelligenza artificiale, che preferiva non imbrigliarne l'evoluzione dell'innovazione tecnologica entro rigidi schemi normativi, si è optato successivamente per il ricorso a strumenti di *soft law*, sino all'impostazione attuale, che ha visto, viceversa, una spinta decisa, almeno nel corso degli ultimi tre anni, verso fonti del diritto di immediata percettività.

Questa tendenza ha visto il continente europeo occupare una posizione di primo piano.

In questo senso, muovono tanto il c.d. *AI Act*, adottato dalle istituzioni dell'Unione Europea nel giugno del 2024, quanto il primo trattato di diritto internazionale dei diritti umani sulla *governance* dell'intelligenza artificiale, approvato dal Consiglio d'Europa nel maggio del 2024, e, cioè, la c.d. Convenzione Quadro in tema di intelligenza artificiale, diritti umani, democrazia e legalità.

L'approccio che ha abbandonato, almeno formalmente, la strategia che lasciava la disciplina dell'intelligenza artificiale nella disponibilità esclusiva di strumenti di *soft law*, non è però rimasto confinato alla sola realtà europea.

Piuttosto, nel corso degli anni più recenti, si è verificata una progressiva espansione della tendenza regolatoria dei sistemi di intelligenza artificiale con una corrispondente erosione degli spazi di discrezionalità della scienza e della tecnica.

Ne costituiscono un esempio importante gli Stati Uniti d'America dove, pure difettando una normativa di livello federale, sono sempre più numerosi gli Stati che stanno legiferando, assoggettando a regole anche stringenti ed innovative le tecnologie di intelligenza artificiale. Tra tutti, si pensi alla legge approvata, ancora una volta nel

2024, dallo Stato del Colorado, il CAIA, che rappresenta il primo tentativo globale di contrasto della discriminazione derivante dall'intelligenza artificiale, la c.d. "discriminazione algoritmica". Colorado che non è rimasto, peraltro, isolato, come dimostrano altri meritori interventi normativi, tra cui la legge entrata in vigore nello Stato del Connecticut sino alle recentissime modifiche che, nell'agosto del 2024, ha apportato al proprio *Human Rights Act* lo Stato dell'Illinois con l'obiettivo di garantire la conformità dei sistemi di intelligenza artificiale ai diritti fondamentali.

Non diversamente, la volontà di non lasciare a sé stesso un fenomeno così pervasivo, tanto nella sfera pubblica quella in quella privata, sta caratterizzando le scelte di molti altri ordinamenti giuridici. È il caso del Brasile, impegnato da alcuni mesi in un serrato dibattito parlamentare che porterà verosimilmente all'approvazione del "*Bill n. 2338 del 2023*" e, allo stato, incentrato sulla opportunità di vietare i sistemi di riconoscimento facciale; alla Cina, all'India, passando per il Giappone e l'Australia.

Non meno rilevanti sono, anche, le opzioni vagliate da Stati non membri dell'Unione Europea, ma europei almeno sul piano geografico, che, però, non hanno ancora sciolto le proprie riserve in favore dell'adozione di una regolamentazione *ad hoc* che irreggimenti l'utilizzo dei sistemi di intelligenza artificiale, ma che non ne sembrano nemmeno così lontani. Sia il Regno Unito che la Svizzera hanno, così, optato per un modello regolatorio alternativo rispetto all'Unione Europea, sebbene non sia da escludere che: l'*AI Act* finirà per riverberare i suoi effetti anche nei confronti di tali Stati, preferendo meccanismi di *soft-law*, da un lato; gli Stati appena menzionati non adottino una propria regolamentazione, come sembra potersi affermare almeno nel caso della Svizzera dove il Consiglio Federale sta studiando le implicazioni collegate ai sistemi di IA con l'obiettivo di presentare una proposta ad inizio 2025.

Continua, invece, a non abbandonare strumenti più morbidi, di *soft-law*, sebbene particolarmente significativi se si considerano la dichiarazione di Toronto e la Carta di Montréal, uno Stato in cui la discussione sulle relazioni tra diritto e intelligenza artificiale è particolarmente avanzato, come il Canada. Canada che, peraltro, nel corso del 2024, sta discutendo della possibile adozione di un proprio *AI and Data Act (AIDA)*, allo scopo di tutelare i singoli individui dalle ricadute pregiudizievoli derivanti dai sistemi di intelligenza artificiale qualificati "ad alto rischio". Una logica, quindi, non dissimile dalla *ratio* alla base dell'*AI Act.*

Se, quindi, a livello globale si assiste ad una convergenza verso la regolamentazione, vi sono alcuni aspetti da segnalare per giudicare la bontà di tali interventi.

Il primo discende dalla valutazione sulla effettiva percettività delle "nuove" leggi sull'intelligenza artificiale. Se, cioè, si assiste ad un *trend* che vuole i sistemi di IA assoggettati a regole di diritto positivo, l'esempio europeo, il primo e il più significativo, lascia, però, aperto più di un dubbio sulla corrispondenza tra gli strumenti predisposti e la finalità di normare l'intelligenza artificiale.

Non casualmente, si è parlato, così, poco sopra di abbandono solo "formale" degli strumenti di *soft law*.

Non si discute la diretta applicabilità entro gli ordinamenti giuridici degli Stati membri e la precedenza rispetto a normative domestiche contrastanti del Regolamento dell'Unione Europea. Ciò che, viceversa, dà adito a qualche perplessità sono piuttosto alcune scelte del legislatore europeo che contraddicono le ambizioni del testo, sotto il profilo sia formale che sostanziale.

Dal punto di vista formale, esiste, in alcuni punti, uno scollamento tra la natura dell'atto, quale fonte del diritto direttamente applicabile e sovraordinata al diritto interno, e i suoi effetti, intesi come capacità del Regolamento di produrre norme giuridiche immediatamente e direttamente percettive, senza intermediazioni o interventi *ex post* dello Stato. Sul piano sostanziale, e quale conseguenza, il Regolamento dimostra poi, spesso, una preferenza per un approccio lasco, che si disinteressa di introdurre norme che guidino gli Stati e gli operatori del settore a rendere conformi i sistemi di IA alle norme regolamentari. Manca, cioè, il passaggio logico ma imprescindibile tra la norma di principio e il "come" realizzare l'obiettivo tratteggiato nel testo.

Si pensi, per tutte, alla norma dedicata alla valutazione del grado di lesività delle tecnologie di IA ad alto rischio. L'articolo 27 dell'*AI Act* pone, infatti, un'obbligazione positiva, cioè la verifica che dai sistemi di IA ad alto rischio non scaturiscano conseguenze pregiudizievoli per i diritti individuali, ma la norma lì si arresta. Non vi sono, tuttavia, indicazioni o criteri precisi sul "come" realizzare la valutazione. E se la norma riconsegna centralità nella fase discendente della normazione di dettaglio agli Stati membri, la conseguenza è il rischio evidente di una risposta frammentata, eterogenea non solo *inter*, ma anche *intra*-statale laddove, al posto degli Stati, saranno le aziende, ciascuna appoggiandosi a canoni propri, a dettare le regole delle "valutazioni di impatto".

Questa apertura a contaminazioni esterne e tra di loro eterogenee, per un verso non consente risposte positive o negative rispetto agli interventi regolatori, perché molto dipenderà dal "come" questi ultimi conosceranno una propria traduzione sul piano normativo nazionale; dall'altro, e volendo osare, la citata incoerenza tra ratio e contenuto delle norme, che rende, in particolare il Regolamento europeo, paragonabile quasi più ad una direttiva, non suggerisce una valutazione del tutto positiva riscontrandosi una incapacità di fondo del testo nel rispondere ai propri obiettivi originari.

Un secondo punto importante, più breve, è dato, poi, dal rispetto del principio della c.d. "neutralità tecnologica" (Cfr., in questo senso, il *GDPR*, § 10 e la *Digital Content and Services Directive* 2019/770), che esigerebbe, qui sì, un meccanismo istituzionalizzato per l'adeguamento delle norme alle ben più rapide evoluzioni della tecnica. Anche qui – si pensi all'allegato del Regolamento europeo sui sistemi di IA ad alto rischio –, l'*AI Act* non sembra rispondere in modo soddisfacente. Esempi, viceversa, più interessanti stanno emergendo oltreoceano. Negli Stati Uniti, la commistione tra azione federale e statale e l'affidamento ad un organismo indipendente di livello federale della gestione degli aspetti che riguardano le potenziali ritorsioni dei sistemi di IA sui diritti fondamentali rappresenta una strategia che sembra meglio rispondere alle esigenze di un approccio neutrale alla tecnologia.

Altrettanto utile richiamare il caso della Svizzera che sta facendo del principio in esame il perno della propria strategia in materia di intelligenza artificiale.

Da ultimo, un terzo profilo investe i rapporti tra le discipline, che vanno affermandosi su scala nazionale e sovranazionale e, cioè, l'esigenza che vi sia una qualche forma di coordinamento che ne assicuri una qualche omogeneità in ragione della caratterizzazione transnazionale del fenomeno dell'intelligenza artificiale. Anche su questo punto, sebbene non siano mancati *summit* internazionali – si pensi, da ultimo, a quello che ha portato alla Dichiarazione di *Bletcheney* del novembre 2023 –, sarebbe auspicabile maggiore attenzione nella definizione di strumenti di raccordo tra i sistemi normativi e di forme di collaborazione tra Stati e organizzazioni internazionali. Un aspetto, tanto più importante soprattutto se posto in relazione al controverso e poco indagato tema – almeno nell'*AI Act* (*contra*, quale esempio meritorio la citata Dichiarazione di Toronto) – della responsabilità (*liability*) per danni scaturenti dall'impiego di sistemi di IA, verosimilmente al centro di prossime azioni giudiziarie dinanzi alle Corti.

In conclusione, non si guarda con sfavore alla regolamentazione dell'intelligenza artificiale di per sé. Sicuramente meritoria è, ad esempio, la messa a punto di principi o criteri "nuovi", che intersecano la realtà giuridica e quella tecnologica: la spiegabilità, la robustezza, la trasparenza, l'affidabilità, il c.d. "*right to know*". Principi, questi sì, condivisi a livello globale.

Ciò che, invece, potrebbe costituire un limite è una tecnica normativa troppo rigida, che poco si raccorda con il *coté* delle scienze informatiche ed ingegneristiche, e che, in definitiva, corre il rischio di divenire velocemente obsoleta, da un lato, e di frenare l'evoluzione tecnologica, dall'altro. Sullo sfondo resta un tema classico dei rapporti tra diritto e innovazione tecnologica e, cioè, l'opportunità di avvalersi di norme elastiche, di agevole adattamento a fattori e condizioni esogene imprevedibili, così da evitare che, anche l'intelligenza artificiale, si trasformi nell'ennesimo caso in cui il diritto e la tecnica non viaggiano allo stesso ritmo.

EDOARDO RAFFIOTTA

Certamente la volontà dell'Unione di intervenire nella regolazione dell'AI in funzione antropocentrica è da salutare con favore, anche per quanto ne deriverà in termini di tutela delle libertà fondamentali e di costruzione di una AI *trustworthy* (con benefici anche per il c.d. *Brussels effect*). Tuttavia, allo stesso tempo, è innegabile che l'AI Act rappresenta, in ordine cronologico, solo l'ultima di numerosissime iniziative messe in campo dall'Unione negli ultimi anni: nell'ambito della costruzione di una "Europa pronta per l'era digitale" abbiamo assistito all'approvazione, tra gli altri, del GDPR; del *Data Governance Act*; del *DSA* e del *DMA*; del *Cybersecurity Act* (nonché di NIS e NIS 2); e potrebbe continuarsi. Una vera e propria *over-regulation* il cui rischio è quello della inevitabile sovrapposizione di competenze e della proliferazione di Organi, Agenzie ed Autorità. Se, insomma, tramite un (ampio) utilizzo delle fonti di

hard law l'Unione ha progressivamente costruito uno spazio regolatorio senza precedenti, nel certamente nobile – e necessario – intento di tutelare i diritti e le libertà fondamentali dei destinatari delle nuove tecnologie, è opportuno in ogni caso non abusarne, e dunque prestare attenzione a non limitare eccessivamente l'operatività dei maggiori (e, a conti fatti, più innovativi) player internazionali.

Certo non è una soluzione facile: spesso lo Stato si dimostra incapace di adempiere al ruolo centrale assegnatogli nel secolo scorso, intrappolato in circostanze che sembrano limitare drasticamente la sua capacità di azione: in un contesto di deregolamentazione, le potenze private potrebbero operare senza restrizioni, portando gli Stati a una posizione subordinata. Al contrario, seguendo la tendenza dell'Unione negli anni recenti, c'è il rischio che lo Stato venga schiacciato dal peso della sua stessa eccessiva regolamentazione. Questo eccesso normativo crea contraddizioni, complica notevolmente il lavoro di chi interpreta le leggi, specialmente i giudici, e compromette la struttura fondamentale del sistema legale, indebolendone l'autorità e la capacità di gestire la complessità della realtà, con conseguenze come la proliferazione di fonti alternative e l'incertezza giuridica.

Nonostante nel contesto attuale il diritto sembri soccombere ai fatti, non è accettabile né possibile abbandonare lo Stato o rassegnarsi all'impossibilità di regolare adeguatamente le tecnologie innovative. Ogni sforzo europeo non dovrebbe prediligere una contrapposizione tra autorità pubblica e influenze private, poiché ciò danneggerebbe l'economia europea, creando ostacoli per le forze innovative fondamentali per la sua sopravvivenza. Inoltre, sarebbe inefficace nel fronteggiare le potenze statunitensi e cinesi.

L'Unione Europea dovrebbe invece utilizzare la sua credibilità e peso economico sulla scena internazionale per promuovere una regolamentazione chiara e basata su principi solidi piuttosto che su complessità burocratiche. Potrebbe realizzare regolamenti e direttive meno complicati e più rapidi da applicare. È cruciale adottare una mentalità pro-innovazione, con un approccio regolatore flessibile, supportato da finanziamenti per la ricerca. La complessità delle tecnologie come l'intelligenza artificiale può essere gestita secondo i propri valori solo se si è attivi nella loro produzione. Secondo l'*AI Index* di Stanford del 2023, gli Stati Uniti restano i maggiori investitori in intelligenza artificiale, con oltre 47 miliardi di dollari nel 2022, più del triplo degli investimenti cinesi e dieci volte quelli britannici, superando anche Germania e Francia. L'Italia non appare nei dati a causa dei fondi insufficienti, ma questi investimenti sono essenziali per sviluppare tecnologie affidabili e competitive, fondamentali per l'economia.

ANDREA SIMONCINI

La scelta dello strumento normativo regolamentare da parte dell'Unione Europea risponde, da un lato, alla finalità complessiva che essa intende perseguire, dall'altro, ad un trend generale della politica normativa dell'Unione.

Sul primo versante, lo scopo fondamentale dell'intervento europeo sull'Intelligenza Artificiale, come sempre in questi settori, è duplice. In primo luogo, fissare alcune garanzie giuridiche essenziali rispetto allo sviluppo ed alla diffusione delle nuove tecnologie visti i rischi che esse comportano, soprattutto rispetto alle libertà fondamentali; in secondo luogo, favorire lo sviluppo e la crescita dell'industria che produce questi medesimi sistemi tecnologici. Per tenere assieme questi "obiettivi gemelli" - come spesso sono chiamati nei documenti europei - un fattore fondamentale, soprattutto per i destinatari produttori di IA, è la certezza e l'uniformità sul territorio europeo della regolazione. Un precedente che sicuramente ha giocato un ruolo importante nella scelta della fonte regolamentare è la vicenda normativa legata alla protezione dei dati personali. Com'è noto, in quel caso, la scelta nel lontano 1995 [Direttiva 95/46/CE] fu quella di utilizzare dapprima la direttiva come fonte, per favorire una certa flessibilità nella attuazione di una normativa così trasversale ed impattante. Ebbene, dopo di 20 anni di applicazione nazionale della "direttiva privacy", si è deciso di re-intervenire con la forma del regolamento (il Regolamento (Ue) 2016/679 noto come *GDPR*), proprio per ovviare ai problemi dei ritardi o delle disomogeneità nell'attuazione dei principi da parte degli stati membri.

L'altra possibile spiegazione di questa scelta è la tendenza generale nel campo delle nuove tecnologie ad adottare la forma regolamentare, accompagnata molto spesso dalla adozione nel titolo della qualificazione - tipicamente anglosassone - di "Act". E' la cosiddetta "Act-ification" della azione dell'Unione [*The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis and EU Law Brutality at Play*, a cura di Vangelis Papakonstantinou e Paul De Hert]; si consideri che oltre all'AI Act c'è il *Digital Services Act*, il *Digital Market Act*, il *Data Act*, il *Data Governance Act*, il *Cyber Resilience Act* e si potrebbe andare avanti. Dietro questa scelta (fonte regolamentare e autoqualificazione di *Act*) ci sono diverse motivazioni: da una generica volontà di sottolineare l'importanza di questi atti normativi, ad una chiara scelta di comunicazione istituzionale, volta a mostrare una Unione Europea estremamente assertiva sul piano regolatorio. La conseguenza più rilevante di questa "inflazione" di regolamenti qualificati come *Acts*, a mio avviso, è che essa contribuisce ulteriormente ad una tendenza già emersa da tempo: quella della progressiva *ibridazione* tra le fonti europee di carattere diretto ed autoapplicativo - come dovrebbero essere i regolamenti - e le fonti a carattere indiretto e non *self-executing* - come dovrebbero essere le direttive -. Infatti, moltissimi di questi regolamenti in materia di tecnologia digitale, ed *in primis* l'*AI Act*, contengono al loro interno norme che non sono in realtà autoapplicative, ma richiedono una necessaria fase di attuazione da parte di altri soggetti, normalmente gli stati membri, ma non solo. È' il fenomeno inverso di quello, altrettanto ben conosciuto, delle cosiddette "direttive *self-executing*" e che fa sì che il regolamento dell'*AI Act*, oltre all'ordinario periodo di *vacatio*, prima di raggiungere la sua piena ed integrale vigenza, richieda una cospicua attività di attuazione e trasposizione interna, essendo composto di norme tutt'altro che integralmente ed immediatamente applicabili, come siamo portati a pensare quando immaginiamo un regolamento e dunque a richiedere un' ampia dilazione temporale (36 mesi)

II Domanda

L'approccio regolatorio basato sul rischio (*risk based approach*) ricorre in tutti gli ultimi regolamenti dell'Unione europea in tema di innovazione digitale. Ritiene che tale approccio risponda alle esigenze del "costituzionalismo digitale"?

FRANCESCA BAILO

L'approccio regolatorio basato sul rischio, che ritroviamo già nel GDPR e che poi è stato preso a modello per gli atti legislativi che sono seguiti in materia di innovazione digitale (sia pur con un sempre più accentuato, anche se non ancora completo, mutamento di prospettiva, da una logica *botton-up* ad una *top-down*) pare rispondere alla sentita esigenza di addivenirsi ad un costituzionalismo digitale europeo, integrandosi con l'obbiettivo di massimizzare la tutela dei diritti fondamentali e, al contempo, garantire e promuovere lo sviluppo di un mercato digitale.

Il ridetto nuovo approccio si propone, cioè, di contenere quelli che sono i più alti rischi connessi all'impiego delle nuove tecnologie, eliminando quelli invece considerabili come rischi "inaccettabili" perché in palese contrasto con i valori e i principi sanciti a livello eurounitario. Tale assetto si pone così in linea di ideale continuità con alcuni atti dell'Unione europea che, pur non avendo natura giuridicamente vincolante, sono risultati particolarmente significativi in quanto produttivi di *policies* che, proprio attraverso questi ultimi atti legislativi, si stanno istituzionalizzando attraverso la formalizzazione giuridica di correlativi diritti e principi.

Tra questi, può, infatti, segnalarsi almeno la "*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*" del 23 gennaio 2023 che, nel mettere al centro della trasformazione digitale le persone, ha sostenuto "la solidarietà e l'inclusione, tramite la connettività, l'istruzione, la formazione e le competenze digitali, condizioni di lavoro giuste ed eque nonché l'accesso a servizi pubblici digitali online", ribadendo "l'importanza della libertà di scelta nelle interazioni con gli algoritmi e i sistemi di intelligenza artificiale e in un ambiente digitale equo", con l'obiettivo esplicito di "costituire un quadro di riferimento olistico" che dovrebbe anche "fungere da punto di riferimento per le imprese e altri soggetti interessati nello sviluppo e nella diffusione di nuove tecnologie" e, particolarmente, per le PMI e le *start-up*. Nella medesima linea, particolare rilievo ha assunto una Risoluzione del Parlamento Europeo sull'intelligenza artificiale nel diritto penale, del 6 ottobre 2021 che, per un verso, ha anticipato la posizione dell'istituzione rispetto all'adozione del successivo regolamento sull'intelligenza artificiale, e, per l'altro verso, è risultata coerente con i principi dettati dalla Carta etica europea sull'intelligenza artificiale nei sistemi giudiziari e nei sistemi connessi, redatta dalla Commissione Europea per l'efficienza della giustizia e approvata

dal Consiglio d'Europa il 3 dicembre 2018. Carta, quest'ultima che, pur collocandosi anch'essa tra gli strumenti di *soft-law*, si rivolge ai legislatori chiamati a regolamentare il quadro prescrittivo entro il quale sviluppare e utilizzare gli strumenti di intelligenza artificiale, aspirando ad assumere un ruolo centrale nella creazione di un quadro normativo e valoriale comune a livello europeo.

È, dunque, anche con detti documenti e, all'evidenza, con i Trattati e con la Carta dei diritti fondamentali, oltreché coi principi sanciti dalla stessa Corte di Giustizia Ue in alcune fondamentali pronunce che hanno creato un vero e proprio *enforcement* della *privacy* digitale nei confronti dell'emergente potere algoritmico. (v., *ex plurimis*, le decisioni del giudice eurounitario sui casi *Digital Rights Ireland*, *Breyer*, *Lindqvist* e *Google Spain*) che il legislatore, negli atti legislativi più recenti, ha dovuto misurarsi per regolamentare le emergenti tecnologie, così come implementate dai poteri pubblici e privati.

Parrebbe, dunque, doversi percepire un processo corale, intrapreso dalle istituzioni europee, nell'adattare e rielaborare le categorie tradizionali del costituzionalismo ad un nuovo ecosistema digitale che tanti mutamenti produce e, verosimilmente, produrrà nell'esercizio e nella stessa garanzia dei diritti fondamentali. Il che, peraltro, impone l'ulteriore sfida, per quello che, dunque, va inteso come costituzionalismo digitale, di cercare di regolare un potere che è distribuito tra molti attori, pubblici e privati, assicurando, al contempo, appropriati limiti esterni all'autonomia di questi sistemi che riflettano le aspettative di legalità tipiche degli ordinamenti democratici, essendo in grado di garantire, sotto il profilo istituzionale, alcuni *standard* di tutela dei diritti fondamentali nonché una distribuzione dei poteri che possa considerarsi equilibrata e coerente con i principi alla base delle tradizioni costituzionali comuni.

Si tratta, tuttavia, di una evoluzione normativa ancora *in fieri* che, talora, non si sottrae ad alcune criticità. Solo per fare qualche sparso esempio, le numerose misure restrittive approntate dal legislatore euronunitario ricadono principalmente sulle *lobbies* delle piattaforme digitali collocate in stati americani e che, dunque, potrebbero avere la capacità economica per opporsi almeno alle limitazioni più radicali introdotte. Ciò senza contare che, soprattutto nel caso delle piattaforme molto grandi, il DSA continua ad assegnare proprio a queste ultime il potere di effettuare gli interventi di moderazione, decidendo quali contenuti ammette e quali rimuovere favorendo, quindi, un potere di autoregolamentazione.

Al contrario, parrebbe da osservarsi con favore la scelta, effettuata nel regolamento sull'intelligenza artificiale, di prevedere dei *sandboxes*, potendo determinare lo sviluppo di un modello di co-regolamentazione tra pubblico e privato capace di ovviare ai difetti di una regolazione tradizionale che, applicata alle nuove tecnologie, apparirebbe inadeguata dal momento che sono le grandi aziende a detenere la gran parte delle conoscenze, ponendosi in una posizione di forza dinanzi ad una regolazione ad appannaggio esclusivo dei poteri pubblici.

GIOVANNA DE MINICO

La regolazione sul modello di quella precauzionale è stata ampiamente sperimentata in Europa in materia di terrorismo, OGM e prodotti pericolosi. Essa intende scongiurare l'accadimento di un evento rischioso con la conformazione della condotta degli operatori a regole comportamentali previamente dettate.

L'*AI Act* introduce un sistema di obblighi cui il fornitore deve conformarsi prima di immettere il sistema nel mercato, che dovranno poi continuare ad essere rispettati dallo sviluppatore sotto la vigilanza di un'autorità di mercato. L'approccio basato sul rischio traduce la tipologia e l'intensità delle regole secondo il canone della proporzionalità, vietando pratiche di IA inaccettabili, stabilendo requisiti per i sistemi di IA ad alto rischio e gli obblighi di trasparenza per i restanti sistemi di IA. [G. DE MINICO, *Libertà virtuali. Costituzione e mercato*, Torino, 2024; M. TUOZZO, *Note intorno al (futuro) Artificial Intelligence Act. Prospettive costituzionali e sfide dell'immigrazione nell'ecosistema digitale*, in *DPER on line*, n. 2/2024].

Tale approccio presenta il vantaggio di concentrarsi sulla riduzione dei rischi più gravi che l'intelligenza artificiale pone alla società [S. HEISS, *Artificial Intelligence Meets European Union Law The EU Proposals of April 2021 and October 2020*, in *EuCML*, n. 6/2021].

Non si può tuttavia trascurare la torsione privatistica che si realizza in tre momenti cruciali.

1) La classificazione dell'alto rischio. L'art. 6 elenca due ipotesi: *a*) i sistemi per i quali esiste una normativa di armonizzazione dell'Unione elencata nell'allegato I, o soggetti a valutazione di conformità da parte dei terzi nei casi, elencati nell'allegato I; *b*) i sistemi adoperati nei settori dell'allegato III (biometria, infrastrutture critiche, istruzione e formazione, lavoro, servizi essenziali, attività di contrasto, immigrazione, giustizia e processi democratici). Rispetto al caso *b*) il testo licenziato all'esito dei trilоghi tra Parlamento, Commissione e Consiglio, ha aggiunto una deroga, confluita nel par. 3 dell'art. 6. Quest'ultimo recita che non è considerato ad alto rischio il sistema che non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale. Tali ipotesi ricorrerebbero quando l'IA esegue un compito procedurale limitato, migliora il risultato di un'attività umana precedentemente completata, non si sostituisce alla valutazione umana, svolge un compito preparatorio ai fini dei casi d'uso elencati nell'allegato III. Il nuovo art. 6 prevede un sistema di *filter clause* che apre a elusioni, sia perché le quattro ipotesi individuate sono troppo generiche; sia perché sono sottoposte ad autodichiarazione. Inoltre, sebbene tale sistema potrebbe essere contemperato dall'iscrizione nel *database* UE, le autorità nazionali – prive di sufficienti mezzi – potrebbero non essere in grado di svolgere adeguatamente il ruolo di supervisione e ri-categorizzare l'IA nell'alto rischio. Il sistema è farraginoso si sarebbe dovuto optare, non per una deroga all'alto rischio con auto-esonero, bensì per la prova in concreto che precede l'immissione sul mercato [P. FRIEDL - G.G. GASIOLA, *Examining the EU's Artificial Intelligence Act*, in *VerfBlog*, 2024/2/07]. Il sistema

vecchio – cioè la clausola generica di assenza di danno significativo – era troppo gravoso e generico per le imprese, ma più garantista per i cittadini perché non bastava la prova da parte dell'impresa che il sistema non recasse rischio significativo ai diritti, ma rendeva necessaria una verifica da parte dell'autorità nazionale di vigilanza. Diversamente, il sistema attuale ha annacquato la *filter clause* non solo perché la prova è *in re ipsa*, ma anche perché l'imprenditore non deve dimostrare nulla, è sufficiente la dichiarazione di esonero che non è sottoposta a un'attività di controllo delle autorità di vigilanza.

2) Il r*isk assesment* sui diritti fondamentali (o FRIA). Esso rappresentava uno strumento positivo introdotto dagli emendamenti del Parlamento europeo di giugno del 2023, depotenziato all'esito dei triloghi perché reso obbligatorio solo per alcuni fornitori. Nello specifico: i soggetti pubblici, i privati fornitori di servizio pubblico, i fornitori di *social scoring* o di assicurazioni sul rischio (art. 27). Si aggiunga poi che la FRIA è a sua volta rimessa all'iniziativa del privato, senza la partecipazione rappresentativa di tutti i soggetti portatori di interessi. Possiamo dire che è un *self and solitary assessment*.

Nel *risk assesment* sui diritti fondamentali c'è infine una nota semi positiva, da un lato la possibilità per i singoli di impugnare il FRIA davanti alle autorità nazionali, cui però non corrisponde un dovere di rispondere al ricorso da parte delle autorità.

3) Il sistema di valutazione della conformità prima di immissione dell'IA nel mercato. Ai sensi dell'art. 43 il fornitore svolge la certificazione *in house* o presso un organismo notificato. Non potrà scegliere con quale delle due opzioni procedere solo: a) qualora non esistano norme armonizzate di cui all'articolo 40; b) il fornitore non le ha applicate o le ha applicate soltanto in parte; c) qualora una o più specifiche tecniche sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione; infine, d) qualora il fornitore ritenga di voler procedere al controllo esterno. Tale sistema di *audit* rimette alla buona volontà del fornitore l'intero sistema di obblighi da rispettare nella progettazione e nell'addestramento del sistema *by design*. Durante i lavori preparatori dell'*AI Act* numerose sono state le critiche sulla scarsa efficacia delle autovalutazioni e degli *audit* a contratto in luogo dei controlli svolti da parte di revisori terzi. Un *audit* solido non solo garantisce i diritti dei cittadini ma facilita gli utenti *downstream*, cioè coloro che costruiranno sulle IA presenti nel mercato ulteriori sistemi [C. DUNLOP, *Policy Briefing. An EU AI Act that works for people and society. Five areas of focus for the trilogues*, 6 September 2023, online al link: *https://www.adalovelaceinstitute.org/policy-briefing/eu-ai-act-trilogues/*].

La promessa di un sistema di IA umanocentrico al momento non sembra essere stata mantenuta perché se da un lato si apprezza un approccio regolatorio *risk based* per i suoi vantaggi, dall'altro la *compliance* al valore della persona è ancora da dimostrare. In questo modo, l'ecosistema di fiducia finisce per reggersi su una catena di presunzioni non controllate e/o che rischiano di evidenziare il loro impatto negativo sui diritti fondamentali oltre il tempo utile alla riduzione dei danni causati dall'IA.

COSTANZA NARDOCCI

L'esigenza di istituire un collegamento tra la nozione di rischio e il diritto, inteso quale insieme di norme preposte a regolamentare, mitigare e contrastare il primo, così come tra rischi e tutela dei diritti fondamentali, si è imposta sulla scena pubblica muovendosi di pari passo con lo spazio, crescente, occupato dalle nuove tecnologie nella sfera pubblica e privata.

Come regolamentare la tecnica e, con essa, i suoi effetti, occasionalmente lesivi di norme di legge e di diritti fondamentali, rimane un interrogativo di fondo per il costituzionalista, così come l'analisi delle tecniche legislative più efficaci. In questo senso, il definito *risk-based approach* rappresenta un'ipotesi di risposta diffusa negli atti normativi più recenti e, così, nell'*AI Act*.

A livello teorico, le difficoltà nel conciliare rischio e diritto, rischi e diritti fondamentali, si devono alla eterogeneità ontologica tra le due nozioni. Se il rischio è quantificabile e tendenzialmente misurabile, il diritto fondamentale si definisce, all'opposto, in base a canoni profondamente diversi ed altrettanto mobili, quali l'etica e la morale letti unitariamente alle qualità socio-culturali di una comunità.

Detta eterogeneità rende complessa ogni regolamentazione, che cerchi di mettere insieme due concetti tanto diversi. Allo stesso tempo, però, lo spazio dei diritti e quello dei rischi è destinato inevitabilmente a sovrapporsi e incrociarsi tutte le volte in cui la violazione dei primi segua il (mal)funzionamento della tecnica, come per i sistemi di intelligenza artificiale.

Non sorprende, allora, che la strategia legislativa del c.d. *risk-based approach* abbia preso il sopravvento per disciplinare i rapporti tra diritti e intelligenza artificiale, il cui impatto sui primi non potrà che misurarsi, appunto, in termini di rischi, identificando il grado o livello di lesività e quantificando, in termini statistici, le probabilità di violazione del diritto fondamentale.

Emblematico di simile approccio è il § 26 del Preambolo dell'*AI Act*, laddove si precisa che: "[a]l fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA […]" (Cfr., anche, l'Art. 5, § 4, TUE).

L'impostazione, che eleva il rischio a criterio pressoché univoco a cui informare la disciplina di determinati fenomeni, non costituisce una prerogativa solamente dell'Unione Europea. Se si volge lo sguardo alle modalità di regolamentazione dei sistemi di intelligenza artificiale diffuse a livello globale, il *risk-based approach* informa, se non tutte, la quasi totalità delle discipline vigenti oppure in fase di adozione. Dalla Convenzione del Consiglio d'Europa alla *Framework for the Classification of AI Systems* dell'OECD, alle proposte vagliate da altri ordinamenti giuridici – gli Stati Uniti, con il *Blueprint* e il primo *Executive Order* dell'amministrazione Biden-Harris, il Canada, il Brasile, per citare i più significativi – ai documenti redatti da alcuni organismi indipendenti, come il *National Institute of Standards and Technology statunitense (NIST)* passando per i documenti internazionali condivisi da alcune

organizzazioni internazionali come nel caso della Dichiarazione di *Blechley* e *dell'International Guiding Principles on Artificial Intelligence (AI) and a voluntary Code of Conduct for AI developers* siglato dagli Stati membri del G7, nessuno ha omesso di ricorrere alla nozione di rischio quale parametro centrale da cui fare dipendere, tra le altre, la scelta di proibire l'impiego di alcune tecnologie di IA oppure di ammetterne l'utilizzo solo in presenza di predeterminate condizioni.

La circostanza che il *risk-based approach* costituisca una impostazione condivisa dalla larga maggioranza dei legislatori domestici e sovranazionali, non rende, però, tra loro sovrapponibili le modalità con cui il rischio e la sua valutazione sono stati, poi, tradotti in norme giuridiche. Non eguali, cioè, sono le possibilità appannaggio del legislatore, che intenda fare uso di simile approccio nella regolamentazione di un fenomeno che espone a pregiudizi i diritti fondamentali.

Da un punto di vista prettamente teorico, occorre premettere che un approccio incardinato sul rischio non contrasta con i principi del costituzionalismo "digitale".

La coerenza tra il primo, l'approccio basato sul rischio, e il secondo, il costituzionalismo "digitale", suggerisce, tuttavia, alcune accortezze e cautele, che consentano di conciliare le differenti *ratio* che soggiacciono alle nozioni di rischio e di diritto fondamentale. In estrema sintesi, ci si riferisce: al rispetto del principio della neutralità tecnologica, che esige il costante adeguamento delle norme giuridiche ai *tempi* della tecnica; alla realizzazione di un'analisi costi/benefici, che scongiuri un astratto o ideologico proibizionismo, che non valorizzi i vantaggi dei sistemi di IA, oppure, che si disinteressi delle loro ricadute pregiudizievoli; all'adozione di una metodologia, che sia *ex ante* chiara, fondata su criteri precisi, identificabili e ripetibili, che consentano la classificazione dei sistemi di IA in base al loro grado di "pericolosità" da indagare anche in dipendenza del settore di utilizzo dei primi; alla preferenza per norme giuridiche flessibili, che favoriscano interventi modificativi o derogatori in attuazione del principio della neutralità tecnologica.

L'interrogativo non è, quindi, se il *risk-based approach* sia o meno conforme al costituzionalismo "digitale". La domanda è, piuttosto, se l'approccio in base al rischio, come interpretato dall'*AI Act*, risponda alle esigenze del costituzionalismo "digitale".

La risposta non è pienamente affermativa per le ragioni che seguono.

La prima.

La preferenza per il *risk-based approach* (in luogo di uno *human rights approach*) male si adatta all'esigenza, pure dichiarata dal legislatore dell'Unione, di tutelare i diritti fondamentali – seppure dopo la sanità e la sicurezza (Cfr. Art. 7, § 1) nelle loro relazioni con le tecnologie di intelligenza artificiale. La valutazione del rischio, proprio per la natura quantificabile e misurabile della nozione di rischio di cui si diceva poco sopra, non si attaglia *de plano* alle caratteristiche del sindacato sulla dedotta violazione di un diritto fondamentale che non risponde a logiche di "misurabilità" o "quantificabilità".

Un diritto, detto altrimenti, o è violato oppure non lo è. Non si pesa la violazione di un diritto fondamentale. Quando si discorre di diritti fondamentali, la sola alternativa che esiste quella tra legalità/illegalità o costituzionalità/incostituzionalità. Non si

discorre di "gradi", più o meno intensi, di violazione di un diritto fondamentale; ragionamento, viceversa, ricorrente se ci si riferisce, all'opposto, come fa l'*AI Act* per i sistemi di intelligenza artificiale, ai rischi che si verifichi "qualcosa". Il rischio, in definitiva, è misurabile da un punto di vista qualitativo, quantitativo e, da ultimo, possono esserne studiate la probabilità, cioè i tempi, di realizzazione. Tutto ciò, per il diritto non esiste. Demandare, quindi, ad un approccio ispirato al solo concetto di rischio la valutazione sul *se* e *quando* i sistemi di IA violano un diritto fondamentale, utilizzando criteri validi per stabilire la ricorrenza del danno, si rivela contraddittoria e, in definitiva, potenzialmente inefficace.

Anche il parametro di riferimento tra rischio e diritto è diverso: collettivo, laddove la verifica riguardi il grado di pericolosità di un sistema di IA, perché il rischio non può essere quantificato se non in base al suo impatto su un gruppo; individuale, quando invece l'oggetto del sindacato è la dedotta violazione di un diritto fondamentale, in quanto tale, di esclusiva titolarità della persona (singola).

In secondo luogo, problematica nell'*AI Act* è l'assenza di un'analisi del rapporto costi/benefici in relazione ai singoli sistemi di intelligenza artificiale, servente rispetto alla successiva decisione di quali tecnologie di IA sono da vietare e, se sì, quando, cioè impiegate *dove*, in *quali* settori. L'*AI Act* non si occupa, infatti, di come i sistemi di IA si comportano in dipendenza della variabile del settore di impiego.

Un terzo aspetto investe, poi, la valutazione astratta del grado di rischio dei sistemi di intelligenza artificiale. L'impostazione *top down*, che fa del legislatore dell'Unione l'arbitro della categorizzazione dei sistemi di intelligenza artificiale in più o meno rischiosi, ammessi oppure da proibire, non sembra poggiare su una robusta evidenza empirica. La preferenza per categorie rigide e astratte rischia di rendere presto obsoleta la normativa europea e non poggia su una valutazione caso per caso dei rischi da associare alle tecnologie di intelligenza artificiale, il cui livello di pericolosità non può essere stabilito a priori ed una volta per tutte e che, al contrario, varia anche in dipendenza del settore entro il quale *quella* specifica tecnologia viene impiegata. Detto altrimenti, un sistema di IA potrebbe essere "ad alto rischio" se utilizzato in un settore e non esserlo se utilizzato per finalità diverse e in contesti altrettanto differenti.

Criticabile è, anche e a monte, l'omessa definizione di che cosa debba intendersi per rischio e di quale sia la soglia dal quale "scatta" l'assoggettabilità ad uno dei quattro gruppi in cui l'*AI Act* classifica i sistemi di IA. Un insieme di aspetti, che rendono discrezionali le scelte del legislatore e, quale conseguenza, incerte le posizioni giuridiche soggettive di coloro che sono e saranno esposti al funzionamento delle tecnologie di intelligenza artificiale.

Da ultimo, quarto punto di criticità, la carente evidenza empirica traspare anche dalla prescelta e troppo ampia nozione di intelligenza artificiale. L'*AI Act* non distingue, come noto, tra sistemi più sofisticati, caratterizzati da un elevato livello di autonomia, come i sistemi *machine learning*, da tutta un'altra vasta gamma di *softwares.* Se a questo si aggiunge che il testo non differenzia, come si diceva, tra sistemi di IA in base al settore e alle modalità di impiego, il pericolo a cui si assiste è l'irragionevole sanzione di sistemi non "ad alto rischio" soltanto perché utilizzati in settori ad alto

rischio e viceversa. Un profilo di irragionevolezza, che richiederebbe di essere preso sul serio dal prossimo intervento della Commissione *ex* art. 6, § 5 dell'*AI Act.*

Per concludere: *risk-based approach* e costituzionalismo "digitale", sì, nella misura in cui siano presi sul serio i diritti fondamentali; *AI Act*, approccio in base al rischio e costituzionalismo "digitale", purtroppo, meno.

EDOARDO RAFFIOTTA

L'approccio regolatorio basato sul rischio ha alcuni punti di forza evidenti, molti dei quali sono in evidente sintonia con la necessità di applicare i principi del costituzionalismo alla nuova era digitale: così, ad esempio, per la protezione dei diritti fondamentali.

Si potrebbe ragionare analogamente anche per quella che è tradizionalmente la funzione-prima del costituzionalismo (limitare il potere costituito, ndr): oggi, la regolamentazione dell'Unione ha il sicuro scopo di voler limitare (o quantomeno rendere controllabile) il potere dei giganti del tech, che certamente hanno acquisito un potere similare a quello di molti Stati tradizionali.

Si inserisce nel solco del costituzionalismo digitale anche la volontà di parametrare la risposta regolatoria in base alle esigenze particolari, e dunque distinguendo tra grandissimi player o situazioni più locali. Risponde anche alle esigenze del c.d. "costituzionalismo digitale". Dobbiamo poi ricordare come una regolamentazione organica ci possa essere d'aiuto nel comprendere come l'uso crescente di internet e delle reti globali influenzi il concetto di sovranità statale e le questioni di giurisdizione.

Nel complesso credo che l'approccio regolatorio basato sul rischio rappresenti una risposta sofisticata e adattabile alle esigenze del costituzionalismo digitale, consentendo di adattare l'intensità delle norme secondo il potenziale impatto su diritti e sicurezza. Il *risk-based approach* è in sintonia con i principi di proporzionalità e flessibilità, elementi chiave per una normativa che deve essere al contempo robusta e dinamica (anche se, a dire la verità, questo aspetto rischia spesso di venire a mancare, per effetto in particolare del discorso di cui sopra).

Concentrare le risorse regolatorie su aree che presentano rischi più elevati permette di proteggere efficacemente i diritti fondamentali senza imporre oneri eccessivi su innovazioni meno problematiche. Tuttavia, la sua implementazione non è priva di sfide: una suddivisione eccessivamente formale e rigida rischia inevitabilmente di avere quale effetto una eccessiva difficoltà interpretativa della norma, andando ad influire negativamente sul fondamentale principio di certezza del diritto.

Ha senso allora interrogarsi sulla possibilità di percorrere strade alternative: è possibile insomma regolare la materia digitale prescindendo da un approccio del rischio (o, comunque, da un approccio del rischio a tal punto articolato e "tecnico")? Un esempio ci viene, forse, dagli USA, e precisamente dalla bozza dell'*Artificial Intelligence Civil Rights Act*: questo nuovo disegno di regolamentazione prescinde infatti da una regolazione spiccatamente *risk-based*, focalizzando invece la propria

attenzione sugli algoritmi che impattano sui diritti civili e sulle opportunità e le libertà individuali (come il lavoro; l'educazione; l'accesso ai servizi), senza – appunto – un approccio *risk-based*.

In sintesi, mentre l'AI Act dell'UE propone un approccio dettagliato e centralizzato per gestire i rischi e le applicazioni dell'AI, le discussioni negli Stati Uniti sembrano più sensibili alle esigenze di sussidiarietà (anche grazie al sistema federale), oltre che incentrate sull'assicurare che l'uso dell'AI non comprometta i diritti civili.

In conclusione forse si possono percorrere anche strade alternative, o – meglio – è possibile una contaminazione tra *risk-based approach* e approcci meno meccanici: una strada percorribile è quella di basarsi su un insieme di principi etici universali che possano fungere da fondamento per lo sviluppo e l'implementazione dell'AI; magari redatti con un accordo tra Stati e soggetti privati: così da istituire un impegno reciproco per valori come la tutela della privacy, l'equità, la non discriminazione e la responsabilità, assicurando che le applicazioni di AI operino nel rispetto dei diritti fondamentali delle persone.

È inoltre imprescindibile stabilire standard tecnologici uniformi che tutte le applicazioni di AI debbano rispettare. Un'altra possibilità è l'introduzione di una certificazione obbligatoria per i prodotti e le applicazioni AI.

Soprattutto, è imprescindibile promuovere un'educazione diffusa riguardo all'AI.

La formazione e la consapevolezza pubblica sono fondamentali per garantire che i cittadini comprendano le potenzialità e i limiti dell'AI e possano partecipare in modo informato al dibattito sulle prescrizioni normative, e diventato tanto più fondamentali quanto più ci si allontana da una categorizzazione di matrice "statuale". In sintesi, una regolamentazione dell'AI che superi l'approccio basato sul rischio può fondarsi su principi etici, standard tecnologici, certificazioni, diritti dei consumatori, monitoraggio attivo e formazione. Questo approccio integrato può contribuire a un uso dell'AI che sia tanto innovativo quanto responsabile.

ANDREA SIMONCINI

Il tema sarebbe molto ampio e mi limito a lasciare aperta qualche domanda. In estrema sintesi, ritengo il "risk based approach" come l'esito del compromesso realizzato in sede europea tra la spinta alla regolazione e l'esigenza delle aziende di non essere eccessivamente vincolate nella propria azione produttiva commerciale. Per questa ragione si è scelto di ricondurre l'IA alla legislazione già esistente sui prodotti pericolosi e sulla certificazione di qualità "CE". Due sono le perplessità principali rispetto a questa scelta sul piano del diritto costituzionale e della tutela dei diritti fondamentali. Innanzitutto, siamo certi che la natura - in sé continuamente in evoluzione - di una tecnologia come l'IA sia del tutto assimilabile a quella di un prodotto (o parte di un prodotto)? Pensiamo alle versioni più recenti della IA cosiddetta "generativa", quella del tipo ChatGpt o Bard per intendersi. In questo caso le possibili applicazioni e gli usi potenziali del "prodotto" AI sono praticamente infiniti. Il Regolamento, in effetti, colto in "contropiede" dall'arrivo di queste nuove soluzioni tecnologiche durante la

discussione nel Parlamento Europeo, ha cercato di inserire nel suo campo di attuazione anche queste ultime versioni, introducendo il concetto di *General Purpose AI*, l'IA *generalista.* Ma anche ad una lettura superficiale del testo è evidente che questa parte risulta essere una "aggiunta" nel corpo della struttura normativa originariamente pensata per l'AI act e originariamente fondata sul "risk based approach". L'ulteriore perplessità sulla scelta di questo approccio nasce dalla considerazione per cui, pur essendo un modello regolatorio abituale e normalmente gradito dai soggetti industriali, l'esito del suo impiego nell'AI Act è stato molto criticato proprio dalla componente imprenditoriale ed industriale. Il noto "rapporto Draghi" sulla è competitività europea [XXX] è stato estremamente chiaro nel richiedere una forte semplificazione del quadro regolatorio cui debbono sottostare le imprese europee, in particolare, nel settore della tecnologia ove occorre procedere ad una netta riduzione del "costo della regolazione". Dunque, anche il *risk based approach*, scelto per favorire il recepimento della regolazione da parte delle aziende, non sembra realizzare a pieno questo scopo. A fronte di ciò, per le nuove e potentissime forme di IA generativa, le uniche precauzioni richieste sono quelle di forme preventive di trasparenza e l'adozione di protocolli di auto-regolazione dinanzi ai cosiddetti - e molto preoccupanti - rischi *sistemici*.

III Domanda
Quali sono, a suo avviso, le novità di maggiore rilievo introdotte dal regolamento?

FRANCESCA BAILO

La novità di maggior rilievo sta probabilmente proprio nell'aver il legislatore europeo voluto, per primo al mondo, normare l'intelligenza artificiale dovendosi, d'altra parte, tener conto che il rigido *framework* normativo che, più in generale, l'Unione Europea ha adottato per porre le fondamenta di una vera e propria "sovranità digitale" si pone in linea di continuità e completamento con quello che è andato modellandosi come un "costituzionalismo digitale", nello spirito di innalzare la protezione dei diritti fondamentali dinanzi alla transizione digitale e, al contempo, affermare una propria autonoma identità rispetto, in particolare alla *governance* al proposito apprestata dai due maggiori *competitor* e, cioè, gli Stati Uniti e la Cina.

Ciò posto, e guardando a quanto più specificamente introdotto, sotto un profilo contenutistico, dal regolamento, possono annoverarsi, tra le novità più importanti: l'ambito di applicazione (soggettivo e oggettivo) e l'istituzione dei *sandboxes*; le pratiche di AI qualificate nella classe di rischio "inaccettabile" e, dunque, bandite e quelle considerate ad "alto" rischio e che, perciò, dovranno attenersi a precise procedure e soddisfare determinati requisiti prima di poter essere introdotte nel mercato; e, infine, il sistema di *governance* "duale" ivi previsto.

Quanto all'ambito di applicazione soggettivo può, infatti, osservarsi che l'art. 2 del regolamento ha una valenza extraterritoriale in quanto si rivolge ai programmatori,

sviluppatori, produttori e fornitori situati negli Stati membri ma si applica pure ai prodotti ivi localizzati, sì da ricomprendere nel perimetro della disciplina tutti quei sistemi di AI che generano un *output* con effetti nel territorio eurounitario. Opzione, quest'ultima, sicuramente inclusiva e che, verosimilmente, sottende la *ratio* di prevenire l'introduzione e la commercializzazione nel mercato europeo di sistemi di AI estere che non rispettino i principi, i valori e i diritti fondamentali sanciti dalla Carta e/o comunque ricavabili dalle tradizioni comuni agli Stati membri. L'ambito di applicazione oggettivo lo si ricava, invece, da quanto disposto dall'art. 1 del regolamento, laddove si dispone che lo stesso stabilisca norme armonizzate per "l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione", da intendersi, ai sensi dell'art. 3, nn. 9 e 10, rispettivamente, come "la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione" e "la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito". Si collocano, dunque, su detto orizzonte applicativo i già richiamati *sandboxes* (v. art. 57 e ss. del regolamento) che, nel creare spazi di sperimentazione normativa al fine di agevolare l'accesso al mercato delle *start-up* oltreché promuovere e sostenere le PMI, consentono ad una pluralità di attori, selezionati sulla base di procedure aperte, di collaborare per apprendere nozioni, progettare, sviluppare e testare nuove tecnologie, in modalità controllata e a basso rischio di violazioni, prima del lancio definitivo dei prodotti. Il che, come già accennato sopra (in risposta al quesito n. 2), potrebbe, più in generale, determinare lo sviluppo di un modello di co-regolamentazione tra pubblico e privato capace di ovviare ai difetti di una regolazione tradizionale.

L'approccio basato sul rischio, al contrario, non può considerarsi una novità ma sicuramente innovativa è la sistematizzazione in classi di rischio e, su questo fronte, di sicuro rilievo sono le norme che riconducono talune pratiche di AI nella classe di rischio "inaccettabile" e che, perciò, non sono immettibili nel mercato europeo. A tal proposito, può osservarsi come il legislatore europeo sia stato attento nell'inserire, esemplarmente, in detta categoria tutti quei sistemi di intelligenza artificiale volti a manipolare, sfruttare ed esercitare un controllo sociale in quanto giudicati dannosi e contrari ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori. Ed è particolarmente sull'impiego dei dati biometrici che viene identificato il crinale tra le attività sicuramente proibite e altre situazioni più complesse che devono essere individuate in modo esaustivo e definite rigorosamente in modo che l'uso dei detti dati sia strettamente necessario per perseguire "un interesse pubblico rilevante", la cui importanza prevalga sui rischi (ad. es. ricerca di vittime del reato, persone scomparse, atti terroristici, localizzazione di autori o sospettati per aver commesso determinati reati ecc.). I sistemi di AI qualificati ad "alto rischio" e che sono puntualmente individuati nell'all. 3, rappresentano, ad ogni modo, la parte più cospicua della normativa e sono soggetti ad un necessario vaglio di conformità atto a provare che questi non ricadano tra i sistemi i cui rischi siano "inaccettabili", oltre a dover essere

concepiti in modo da poter essere sorvegliati in modo efficace da persone fisiche nel corso del loro utilizzo. Sorveglianza umana che, peraltro, se da un lato produce un senso di fiducia ed affidabilità, dall'altro pare un concetto maggiormente sfuggente dal momento che l'AI, sfruttando metodi di apprendimento automatico basati sull'esperienza, rende arduo un tale tipo di controllo, mancando una concreta prevedibilità degli esiti a cui l'AI potrebbe condurre.

Da ultimo, l'assetto, articolato e complesso, della *governance* risulta di fondamentale rilevanza in quanto è stato prevista l'istituzione sia di un organismo di carattere sovranazionale, il Comitato europeo per l'Intelligenza Artificiale che sembrerebbe strutturarsi in modo analogo all'EDPB già previsto nel GDPR, sia di un organismo avente una connotazione nazionale ma saranno i singoli Stati membri a dover designare una o più autorità competenti. È stato poi attribuito al Garante europeo per la protezione dei dati la competenza a sindacare l'operato delle Istituzioni, delle Agenzie, degli organi dell'Unione quando rientrino nella portata applicativa del Regolamento e, in caso di eventuali situazioni di inadempienza e di irregolarità, lo stesso avrà il potere di irrogare sanzioni pecuniarie nei loro confronti.

COSTANZA NARDOCCI

Oltre il merito e ai punti critici, l'*AI Act* rimane la prima regolamentazione dei sistemi di intelligenza artificiale, che abbia trovato compiuta realizzazione a livello globale.

Più che nei contenuti, l'aspetto, quindi, più innovativo del testo si coglie nella stessa scelta delle istituzioni dell'Unione Europea di assoggettare ad un Regolamento il fenomeno dell'intelligenza artificiale, garantendo al contempo l'ambizioso scopo di garantirne l'omogenea applicazione entro i confini degli Stati membri.

Di segno differente è stato, viceversa, l'approccio degli Stati Uniti, così come del Regno Unito, della Cina. A livello federale, gli Stati Uniti rimangono, così, ancorati ad un modello di *soft law*, lasciando agli Stati ampio margine di intervento, come si sta verificando negli ultimi anni e, in modo più significativo, nel corso degli ultimi mesi (Cfr. le leggi approvate dallo Stato del Colorado, del Connecticut, della California, nonché i recenti emendamenti apportati dallo Stato dell'Illinois al proprio *Human Rights Act*), che hanno assistito al rapido incremento del numero di leggi in materia di intelligenza artificiale, che si stanno affiancando al già citato *Blueprint for an AI Bill of Rights* e, soprattutto, al precedente *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.*

Da altra angolazione, se non è innovativo entro i confini europei, il ricorso al c.d. *risk-based approach*, quest'ultimo costituisce, invece, profilo da segnalare in prospettiva sia comparata che globale, perché distanzia l'*AI Act* da coeve esperienze o tentativi regolatori.

L'esperienza statunitense rappresenta ancora un esempio emblematico. Se l'*Executive Order* dell'amministrazione Biden-Harris si prefigge di assicurare un

utilizzo sicuro dei sistemi di intelligenza artificiale, sostanzialmente diversa è la traduzione della *ratio*, cioè dell'approccio al "rischio", nei due testi. L'*AI Act* opta per una definizione astratta ed *ex ante* delle tecnologie di IA a rischio, disinteressandosi del relativo ambito di utilizzo. L'*Executive Order* non riposa, viceversa, su rigide categorizzazioni predeterminate, preferendo incentrare le proprie raccomandazioni sul combinato disposto tecnica di IA/settore di impiego, nel tentativo di gestire, se *ex post* rimane poco chiaro, i rischi dei sistemi di IA in rapporto alle specifiche ricadute applicative studiate per ambito di azione.

Un terzo elemento innovativo del testo europeo è, poi, rintracciabile nella altrettanto criticata, ma pur sempre "nuova", opzione in favore di un'interpretazione dell'approccio al rischio, secondo la prospettiva *top down*. A differenza degli altri atti normativi dell'Unione, che pure ripiegano sul criterio del rischio, l'*AI Act* rafforza l'impostazione "dall'alto", rendendo il legislatore dell'Unione primo ed unico artefice delle scelte più controverse e complesse. Tra queste, le principali risiedono: nella selezione delle tecnologie di intelligenza artificiale considerate "ad alto rischio", elencate nell'*Annex III*; nella delimitazione delle tecnologie da vietare perché ree di porsi all'origine del c.d. "*unacceptable risk*"; ancora, nella definizione delle eccezioni al divieto di ricorso a specifici sistemi di intelligenza artificiale. Un esempio per tutti è costituito dal ritenuto legittimo impiego delle tecnologie di identificazione biometrica, quando ciò si renda necessario per rispondere ad esigenze di difesa oppure di sicurezza pubblica nazionale.

Un quarto aspetto innovativo, sempre oggetto, tuttavia, di qualche perplessità quanto al merito, è costituito dalla nozione di intelligenza artificiale. Il legislatore dell'Unione Europea ricalca la proposta definitoria dell'OECD, ma, al tempo stesso, ne estende la riferibilità a tecnologie di tipo diverso. È il caso, già richiamato, dei semplici *softwares* oppure di tecnologie di IA non *machine learning*, che l'*AI Act* pone sotto l'ombrello del concetto di "intelligenza artificiale", riferendovi analoghi requisiti di *compliance*.

Da ultimo, pure non abbracciando una impostazione *human-rights based* per le ragioni che si è evidenziato poco sopra, l'*AI Act* è stato, ciò nonostante, il primo a tradurre in obbligazione giuridica l'esigenza di procedere ad una valutazione di impatto dei sistemi di intelligenza artificiale sui diritti fondamentali. Il problema, se mai, è che l'intuito del legislatore dell'Unione è rimasto sulla carta, omettendo l'*AI Act* di fornire indicazioni concrete sul "come" tradurre in pratica l'obbligazione in esame. Il risultato è stata la circolarità del modello europeo, ma anche il suo superamento da parte di chi è arrivato prima nel proporre linee guida, che orientino la valutazione di impatto. Si pensi: agli Stati Uniti con le strategie messe a punto dal NIST nel proprio *Assessing Risks and Impacts of AI (ARIA) Pilot Evaluation Plan*, pubblicato nel mese di agosto 2024; al Regno Unito con il *Artificial Intelligence Impact Assessment (AIIA)*, messo a punto dal *RAI Institute*; al Canada con l'*Algorithmic Impact Assessment Tool*, che costituisce un vero e proprio prodotto di indagine del livello di rischio prodotto dai c.d. *automated decision-systems*.

Il superamento non è soltanto formale o temporale. Interessanti sono, infatti, alcune scelte che investono la sostanza della disciplina come alcune scelte proposte in tema di responsabilità. Il tema della *liability*, che l'*AI Act* circoscrive alla figura dell'utilizzatore finale (*deployer*), è, invece, estesa da alcune proposte regolatorie e leggi vere e proprie, al ricorrere di specifiche circostanze, anche al programmatore secondo un modello di responsabilità condiviso, che pone in capo ad entrambi i soggetti una serie di obbligazioni che seguono al ruolo assolto nella ideazione, funzionamento e messa in atto dei sistemi di IA (Cfr. la legge dello Stato del Colorado, il CAIA, di cui *supra*).

Forse, ironicamente – perché non necessariamente "novità" non è sinonimo di "bontà" –, l'aspetto innovativo dell'*AI Act* risiede: nell'aver offerto, per primo a livello mondiale, una proposta di regolamentazione dei sistemi di intelligenza artificiale ad ampio spettro, che poggia su norme di diritto positivo; nelle modalità, con cui il legislatore dell'Unione Europea ha interpretato il criterio rischio, secondo una lettura *top down*, inedita anche agli altri testi normativi dell'Unione; nella opzione in favore di un concetto ampio, forse troppo di intelligenza artificiale, che assoggetta alle stesse regole sistemi diversi e dalle parimenti eterogenee e variabili implicazioni.

EDOARDO RAFFIOTTA

Probabilmente dal punto di vista tecnico una delle maggiori novità è rappresentata dalla c.d. FRIA, *ex* art. 27 *AI Act*; anche perché come noto non era prevista nelle prime versioni/bozze del Regolamento: oggi l'articolo 27, rubricato "Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio", richiede ai soggetti responsabili del dispiegamento di tali sistemi di effettuare "una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema potrebbe comportare" prima della loro implementazione (l'articolo è incluso nelle parti dell'*AI Act* che entreranno in vigore 24 mesi dopo la pubblicazione del Regolamento nella Gazzetta Ufficiale, quindi a partire dal 12 luglio 2024). Nella proposta iniziale presentata dalla Commissione Europea nel giugno 2021, non era contemplata la valutazione d'impatto sui diritti fondamentali: l'inserimento di questo strumento nel Regolamento è stata invece una diretta conseguenza dei negoziati che hanno avuto luogo nelle sessioni di trilogo tra la Commissione europea, il Consiglio dell'Unione Europea e il Parlamento Europeo. È stato infatti un emendamento del Parlamento che ha permesso per la prima volta di includere la FRIA nell'allora articolo 29a; mantenendo poi tale previsione sino a farla divenire parte dell'accordo provvisorio raggiunto il 9 dicembre 2023. Meno "innovativa" è la *ratio* cui risponde la FRIA: l'introduzione di una norma specifica sulla valutazione d'impatto dei diritti fondamentali si inserisce infatti in un contesto di crescente attenzione da parte dell'Unione Europea verso le conseguenze e le potenziali ripercussioni dei sistemi di AI ad alto rischio sui diritti e le libertà individuali, facendo sì che il Regolamento possa essere visto come la naturale prosecuzione delle linee tracciate dal Libro bianco sull'AI e dei principi etici per un'intelligenza artificiale

affidabile, elaborati nel 2019 da un gruppo di esperti indipendenti designati dalla Commissione. L'obiettivo dichiarato è quello di sviluppare un'IA che sia quanto più affidabile possibile per gli esseri umani. Pertanto, non sorprende che, per raggiungere tale scopo, si sia optato per l'adozione di strumenti di valutazione d'impatto già sperimentati e sostenuti da vari protagonisti del settore, tra cui il Parlamento Europeo, legislatori, accademici e rappresentanti della società civile.

ANDREA SIMONCINI

Sono moltissime le novità rilevanti, ma penso che quella che può incidere più profondamente nello sviluppo futuro dell'IA è la previsione contenuta nell'art. 10 del regolamento, intitolata *Dati e Governance dei dati*. Con questa norma per la prima volta si pone una disciplina che riguarda direttamente una delle attività fondamentali per la creazione degli algoritmi di IA: il cosiddetto "machine learning". Gli algoritmi di IA com'è noto, a differenza dei sistemi di programmazione per così dire "classici", vengono realizzati attraverso tecniche di addestramento automatizzato che prevedono l'impiego di grandi quantità di dati di training. I modelli di AI che vengono creati dipendono, dunque, non solo da chi progetta l'architettura del sistema di addestramento ma, in questi casi soprattutto, dal *tipo* di dati che vengono utilizzati per far "apprendere" la macchina. Uno degli esempi più noti in questo campo deriva da un primo notissimo caso giudiziario americano, in cui un giudice ha utilizzato un sistema di IA per stabilire la pericolosità sociale di un imputato. Il programma in questione - il famoso software COMPAS - essendo stato addestrato su un data-set costruito sulle storie personali di coloro che si trovavano in prigione negli Stati Uniti, aveva finito per "imparare", ma in maniera distorta e, dal momento che la stragrande maggioranza dei prigionieri nelle carceri americane è composta da persone di colore, finiva per produrre previsioni errate e discriminatorie sulla base del colore della pelle. Per questo motivo l'AI act prevede che "*i sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi (...)*". Ovvero vengono stabiliti dei requisiti di qualità per i dati che sono impiegati per addestrare gli algoritmi. Quali sono questi requisiti? L'art. 10 richiede che "*i set di dati di addestramento, convalida e prova sono soggetti a pratiche di governance e gestione dei dati adeguate*", ponendo così in capo ai produttori e agli utilizzatori di IA un obbligo di adozione di tecniche di "gestione e governance" dei dati adeguate, trasparenti e soprattutto, corrette. Prosegue, infine, l'art. 10 affermando che "*i set di dati di addestramento, convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai quali il sistema di IA ad alto rischio è destinato a essere usato*."

Questa norma, come dicevo, è rivoluzionaria perché responsabilizza i programmatori e i produttori di IA nei confronti dei dati che usano per creare i propri sistemi algoritmici. Sinora abbiamo assistito ad una totale opacità sui data-set impiegati; soprattutto per la disponibilità apparentemente gratuita del più ampio e non controllato database mai concepito: Internet e i social media. È sui dati di Internet e su quelli dei social media che sono stati costruiti tantissimi moltissimi dei sistemi di IA predittiva oggi in commercio e che, una volta applicati, hanno mostrato chiarissimi segni di *bias* e di discriminazione. Anche i cosiddetti Large Language Models - quelli utilizzati per costruire l'IA generativa del tipo Chat-Gpt - sono stati addestrati prevalentemente su quella enorme banca dati, facilmente disponibile ma del tutto arbitraria, incompleta e piena di contenuti discutibili che è la Rete web. Per questo porre il principio per cui "i *data-set di addestramento convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista*" rappresenta un grande passo in avanti nella internalizzazione della protezione giuridica dei diritti *by design*, sin dal disegno del progetto di *machine learning*.

Va anche osservato, però, che questo articolo è uno di quelli che i rappresentanti dell'industria tecnologica hanno maggiormente criticato, sostenendo che il rispetto di questi criteri è particolarmente gravoso per chi sviluppa software di questo genere e che un data-set composto solo di dati pertinenti, rappresentativi ed esenti da errori, sarebbe - praticamente - impossibile. Sarà decisiva sul punto l'attuazione del regolamento e i sistemi di accreditamento che verranno elaborati per i sistemi di IA ad alto rischio.

IV Domanda

Tra i settori ad alto rischio previsti dall'allegato 3 del regolamento, quali potranno trarre i maggiori benefici dall'utilizzo dell'intelligenza artificiale?

FRANCESCA BAILO

È forse ancora prematuro potersi esprimere circa l'individuazione dei settori ad alto rischio che potranno trarre i maggiori benefici dall'utilizzo dell'intelligenza artificiale ma si può immaginare che, tra questi, potrebbero rientrarvi le infrastrutture critiche, ossia quei "sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità", ma poi anche le "attività di contrasto" e, infine, l'amministrazione della giustizia, purché le ridette tecnologie innovative vengano impiegate a supporto (e non in integrale sostituzione) dell'attività umana, siano sottoposte ad una sorveglianza efficiente ed efficace da parte della persona fisica e non siano in contrasto con i diritti fondamentali garantiti a livello eurounitario, in ottemperanza a quanto sancito dal regolamento.

Specie in relazione all'amministrazione della giustizia può osservarsi come, in una prospettiva comparata, è stata maturata una certa esperienza nell'uso dell'intelligenza artificiale che certamente ha fornito e/o potrebbe fornire spunti, anche normativi, per affinare e, laddove necessario, massimizzare la tutela dei diritti fondamentali che potrebbero risultarne "stressati".

In questo senso, può essere, esemplarmente, ricordato che nel caso *Loomis* la Corte Suprema americana ebbe a sostenere la discrezionalità del giudice nel valutare gli esiti di un algoritmo, preservandone però i diritti di proprietà intellettuale malgrado questo fosse risultato poi discriminatorio e, comunque, non trasparente, come dimostrato da successivi studi condotti da una Ong.

Più recentemente, inoltre, è invalso, sia tra i giudici, sia tra gli studi legali, l'impiego di *ChatGPT*, avendo alcuni giudici apertamente dichiarato di essere stati supportati da detta tecnologia nel decidere (v., ad es., i casi colombiani di gennaio 2023, il caso peruviano di marzo 2023 ma altri casi stanno capillarmente emergendo: sul punto, v., *amplius*, E. LONGO, *La "Giustizia digitale" tra nuove forme di efficienza e garanzia dei diritti costituzionali*, in *La nuova giuridica*, 2023, 187-209) mentre, com'è noto, è stato proprio un giudice americano a sanzionare pesantemente uno studio legale per aver citato nei propri atti di difesa casi giurisprudenziali del tutto inventati dalla ridetta tecnologia. Sul versante nazionale occorre, inoltre, ricordare che il garante per la protezione dei dati personali, con provvedimento d'urgenza del 30 marzo 2023, ha limitato temporaneamente (v. il successivo provvedimento dell'11 aprile 2023, che ha sospeso l'efficacia dell'ordine cautelare) l'utilizzo in Italia del citato *software* in mancanza di una informativa agli utenti e a tutti gli interessati i cui dati venivano raccolti dalla fornitrice, l'impresa *OpenAI*, oltreché in assenza di una base giuridica che giustificasse la raccolta e la conservazione massiccia di dati personali, allo scopo di "addestrare" gli algoritmi sottesi al funzionamento della piattaforma. Ancora diversa è stata la posizione delle corti gallesi e inglesi, in cui il livello di digitalizzazione del processo si è già consolidato ed è stata più di recente adottato una Guida, redatta dai giudici di vertice, per assistere i titolari degli uffici giudiziari nell'uso dell'AI. Con riguardo ai sistemi di profilazione dei giudici, particolarmente dirimente è stata la decisione del *Conseil Constitutionnel*, (dec. n. 778-2019), con cui è stato dichiarato conforme al dettato costituzionale l'art. 33 della Loi. n. 2019-222 nella parte in cui vieta ai ricorrenti di utilizzare i dati identitari dei giudici.

Rispetto alla rapida casistica ora richiamata da parte per lo più di ordinamenti non facenti parte dell'Ue, può osservarsi come l'AI Act abbia il pregio di porre fine ad un certo lassismo nell'impiego anche in detto settore delle più potenti tecnologie, con l'obiettino di armonizzarne la disciplina e, al contempo, innalzare la tutela dei diritti fondamentali coinvolti, nell'auspicio che detti sistemi possano essere usati, così come richiesto dal regolamento, in modo responsabile e proporzionato e che possano recare tra i benefici, una minor durata dei procedimenti giurisdizionali, un supporto o ausilio al processo decisionale, nonché un'agevolazione nell'accesso da parte dei cittadini alla giustizia.

GIOVANNA DE MINICO

Tra i settori di alto rischio l'amministrazione della giustizia (punto 8 dell'allegato III) sembrerebbe trarre significativi benefici dall'utilizzo dell'intelligenza artificiale o, meglio, dalla regolazione delle sue modalità di ingresso nel processo. L'All. III, al n. 8, recita che l'IA è destinata "ad assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti…".

Quest'affermazione può sembrare in prima battuta contraria a quella che io ritengo sia una pretesa irrinunciabile dell'uomo: il diritto a essere giudicato da un giudice umano. Esigenza che ha una duplice giustificazione: la dignità del giudicando, il quale ha fiducia solo nella valutazione proveniente da un suo simile; la parità tra uomini: il giudice non è *legibus solutus*, anche lui un giorno potrebbe sedere al banco degli imputati, il che lo induce a comportarsi come vorrebbe che si comportassero nei suoi confronti.

Il *framework* costituzionale di riferimento è composto dalle norme (artt. 101, co. 2 e 104 Cost.), che proteggono l'autonomia decisoria del giudice, intesa almeno nei termini della sua equidistanza dalle parti, e l'indipendenza, cioè il non dover prendere ordini da nessun potere dello Stato, come da nessuna delle parti processuali, perché i giudici sono sottoposti solo alla legge.

Dal mio punto di vista è dunque quantomai opportuna l'impostazione dell'*AI Act* che ammette un ingresso della mente meccanica in posizione ancillare, e non sostitutiva, alla *iurisdictio*. Essa conferma la collocazione della mente meccanica nel dialogo con la funzione giurisdizionale all'interno del modello di intelligenza ad alto rischio, con tutto ciò che segue in termini di disciplina precauzionale applicabile.

Ebbene, assistere significa aiutare sempre che l'aiutato lo voglia e quindi il giudice non è obbligato ad avvalersene, altrimenti il legislatore europeo sarebbe ricorso a un altro verbo.

Diversamente un ingresso dell'IA più penetrante nel processo ostacolerebbe non solo l'autonomia costituzionale, ma anche l'adattamento evolutivo del diritto.

L'ingresso dell'intelligenza predittiva finirebbe per influenzare e assorbire ogni energia volitiva del giudice, al punto che questi sarebbe costretto in difesa della sua discrezionalità decidenti ad assumersi un onere motivazionale più pesante di quello che di regola sopporta quando agisce in assenza del contribuito meccanico. Il giudice dipenderebbe dalle risultanze tecniche, il che lo ridurrebbe in uno stato di soggezione, che di per sé viola il dettato costituzionale, che lo sottopone alla sola legge; infatti, il giudice non tollera padroni diversi dalla volontà astratta e generale del legislatore. Il suo unico termine di confronto è il parametro normativo, essendo tenuto a un'attività di *iurisdictio*; se invece dovesse motivare le ragioni del suo dissenso rispetto all'esito meccanico, il giudice avrebbe due parametri cui attenersi nel giudizio: normativo e tecnico. L'unico beneficio di questa contaminazione sarebbe la certezza giuridica e la prevedibilità del diritto [U. RUFFOLO, *Giustizia predittiva, decisione algoritmica e ruolo ancillare della machina come ausiliare necessario del giudice umano*, in A. PAJNO - F.

DONATI - A. PERRUCCI (a cura), *Intelligenza artificiale e diritto: una rivoluzione?*, vol. II, Bologna, 2022]. Dall'altro canto, ciò azzererebbe l'interpretazione evolutiva del diritto, che senza scivolare nell'attività creativa di nuove norme, consente invece al tessuto regolativo, suscettibile di letture non univoche, di adeguarsi in maniera costante e ininterrotta ai mutamenti della realtà. La sentenza algoritmica potrebbe solo replicare per l'avvenire quanto accaduto nel passato secondo una logica di tipo statistico [C. CASONATO, *Giustizia e intelligenza artificiale: considerazioni introduttive*, in *BioLaw Journal – Rivista di BioDiritto*, 2/2021]. Si farebbe così strada un modello di diritto riducibile a un mero calcolo matematico, dall'esito certo e incontrovertibile, "acquisibile e pienamente calcolabile proprio in ragione della sua riducibilità a computo matematico" [M. LUCIANI, *La decisione giudiziaria robotica*, in *Rivista AIC*, n. 3, 2018. Sulla calcolabilità G.W. LEIBNIZ, *Principi ed esempi della scienza generale*, in F. BARONE (a cura di), *Scritti di logica*, Milano, 2009]. In questo quadro di univocità interpretativa che non lascia spazio alla discrezionalità, è utile domandarsi in che modo dovrà essere svolta l'attività di *legislatio* quando il "giudice deve chiudere norme aperte, ad esempio, quelle che rinviano alla buona fede o alla diligenza, con la conseguenza che la disposizione potrà essere applicata al caso concreto solo dopo essere stata completata. Nelle discipline settoriali il corretto rapporto tra legislatore e giudice addirittura si inverte con il secondo che sta in luogo del primo: si pensi alla legislazione *antitrust*, nazionale ed europea, interamente composta da fattispecie a formazione progressiva, che si perfezionano solo con l'apporto volitivo, non meramente accertativo, delle Autorità antitrust e dei giudici" [G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, 2/2024, 100].

Solo una intelligenza artificiale "constitutional by design" [G. DE MINICO, *Towards an "Algorithm Constitutional by Design*", in *BioLaw Journal – Rivista di BioDiritto*, 1/2021, in part. par. 6] potrà rispettare l'azione di regolamento dei confini tra il supporto predittivo, operante su base statistico-meccanica, e l'azione cognitivo-valutativa del giudice, che si articola in base al nesso di causalità e senza vincoli di ripetibilità di ciò che è accaduto nel passato in modo da favorire una maggiore elasticità della *iurisdictio* e a sostenere l'azione propulsiva verso la flessibilità regolatoria.

Occorre tuttavia integrare l'All. III con il catalogo dei diritti dell'AI Act per dare effettività all'attività giudiziaria a guida umana, garantendo al cittadino l'accesso alla spiegazione dell'*output* uscito dal processo. Solo un catalogo di diritti orientato alla trasparenza potrà svelare l'opacità di una tecnologia inintelligibile e rendere contestabile la decisione algoritmica, che si nasconde dietro l'alibi dell'oggettività e della certezza scientifica al solo fine di godere del privilegio dell'immunità giuridica [G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, cit., 93]. Nella domanda n. 5 mi soffermerò su questi aspetti.

COSTANZA NARDOCCI

La domanda che qui si pone risulta di non agevole risposta.

E non lo è, essenzialmente, per le deroghe o eccezioni, che il Regolamento dell'Unione Europea ha disposto in relazione alla categorizzazione e, quale riflesso, all'utilizzo delle tecnologie di IA pure qualificate, *ex ante*, "ad alto rischio".

Ci si riferisce, in particolare, alla deroga, di ampia portata applicativa, che consente il ricorso a sistemi di IA "ad alto rischio", in presenza della attestazione che ne dimostri la non lesività rilasciata dalle organizzazioni e dalle aziende, che intendano farne uso di una tecnologia di IA che presenti i requisiti di cui all'art. 6, § 1, dell'*AI Act* oppure che rientri nel novero di quelli elencati dall'Allegato III *ex* art. 6, § 2.

Il paragrafo 3 dell'art. 6 dell'*AI Act* precisa, infatti, che "[i]n deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale". E questa è la prima condizione.

A detta previsione, si affiancano, poi: i criteri – certamente carenti quanto a determinatezza e precisione –, in base ai quali deve considerarsi non "ad alto rischio" taluni dei sistemi di IA elencati a norma delle lettere a, b, c, d.; e la norma, forse più importante, che rimette all'utilizzatore finale la possibilità di utilizzare un sistema di IA "ad alto rischio", laddove sia in grado di provarne la non lesività. Il § 4 dell'art. 6 stabilisce, infatti, che: "[u]n fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio".

La lettura unitaria dei paragrafi dell'art. 6, che ammettono deroghe al divieto di utilizzo dei sistemi di IA "ad alto rischio", sollecita qualche perplessità in ordine alla effettiva capacità dell'*AI Act* di definire in modo tassativo quali siano i sistemi di IA "ad alto rischio" e, cioè, da vietare, sempre.

In secondo luogo, la norma che demanda all'utilizzatore la possibilità di sottrarsi ai divieti in discorso sulla base della mera produzione di una valutazione discrezionale sulla non pericolosità del sistema di IA e, quindi, sulla sua non inquadrabilità nel novero di quelli "ad alto rischio", genera una estrema varietà e frammentazione di soluzioni, perché eterogeneo sarà il contenuto di tali valutazioni così come le risposte sul livello di lesività di ciascuna tecnologia di IA presa in considerazione; una frammentazione, destinata a prodursi sia nei rapporti tra gli Stati membri, sia e, soprattutto, all'interno dei singoli ordinamenti giuridici, poiché sarà la singola azienda (o organizzazione), in quel dato caso di specie, a produrre la documentazione *ex* art. 2, § 4.

Se questo è il contesto, comprendere a priori quali saranno gli ambiti che trarranno maggiore beneficio dall'intelligenza artificiale si rivela particolarmente complesso.

Se, però, uno dei principali problemi è costituito, come detto, dalle conseguenze negative, soprattutto sul piano della certezza del diritto, che discendono dalle eterogenee valutazioni degli utilizzatori sulla pericolosità del sistema di IA, potrebbe almeno sostenersi che, i settori dove esiste meno frammentazione in termini di minore concentrazione di potenziali soggetti a cui l'*AI Act* rimette l'obbligo di produzione della documentazione *ex* art. 6, § 4, si vedranno esposti ad un rischio minore di aggiramento

delle previsioni del Regolamento europeo. Rischio, da intendersi qui come probabilità di immissione nel mercato di tecnologie di IA che, al di là di che cosa dichiara l'organizzazione oppure l'azienda, impattano negativamente sulla salute, sulla sicurezza e sui diritti fondamentali e che, cioè, sono a tutti gli effetti "ad alto rischio". In questi settori – un esempio potrebbe essere costituito forse dall'amministrazione della giustizia (ma, forse, in futuro, dipenderà dalla organizzazione dei singoli uffici giudiziari) –, sarà parimenti ridotta l'incertezza giuridica, che allo stato caratterizza la identificazione dei sistemi di IA "d alto rischio" e la loro separazione rispetto a quelli che, viceversa, non lo sono. Discorso opposto vale per il settore lavoristico, dove elevata è la frammentazione tra imprese, aziende, organizzazioni con relative e diversificate risposte in punto di pericolosità dei sistemi di IA che si vogliano qualificare non "ad alto rischio".

Vi è, inoltre, da aggiungere che è evidente che, laddove maggiori saranno le possibilità di fare ricorso alle deroghe di cui sopra, in ragione ad esempio della loro più o meno intensa privatizzazione, minori saranno probabilmente i benefici da trarre dai sistemi di IA. Qui, la prospettiva che si accoglie subordina il "beneficio" o i benefici del ricorso ad un sistema di IA al previo ed inderogabile rispetto dei diritti fondamentali. Ne discende che, più numerose saranno le probabilità di elusione dei divieti di uso di tecnologie di IA "ad alto rischio", anche in ragione delle lacune o imprecisioni del Regolamento, minori saranno i "benefici" per la collettività e per i singoli.

Difficile anche parlare pacificamente di "benefici" con riferimento a tutte le ipotesi in cui l'*AI Act* ammette l'utilizzo, da parte delle forze dell'ordine, degli strumenti di IA forse più controversi e, cioè, dei sistemi di identificazione biometrica. Se l'impiego, come noto, soggiace ad esigenze di sicurezza pubblica, è altrettanto importante considerare che, di fronte ad una giurisprudenza sinora carente quanto alle relazioni tra sistemi di IA e diritti fondamentali, la porzione più consistente riguarda proprio l'utilizzo dei sistemi di riconoscimento facciale su cui pure la Corte europea dei diritti dell'uomo ha avuto modo di pronunciarsi di recente (Cfr. Corte EDU, *Glukhin c. Russia*).

Di fronte a un quadro tanto complesso e all'impossibilità, a parere di chi scrive, di stabilire aprioristicamente quali saranno i benefici e "dove" si produrranno, resta da mettere l'accento su due aspetti.

Il primo è che tali carenze e criticità del Regolamento, quanto alla chiara delimitazione delle tecnologie "ad alto rischio", derivano proprio dall'approccio non settoriale dell'*AI Act*, che decide e classifica a monte quali tecnologie di IA sono "pericolose", senza tenere conto di quanto tale valutazione sia influenzata dalle circostanze di utilizzo dell'intelligenza artificiale e della altrettanto rapida evoluzione di tali tecnologie che dovrebbe suggerire norme, come già detto, tecnologicamente neutrali e che non ripiegano su elenchi di divieti e di eccezioni alla regola.

Il secondo investe, invece, la posizione delle aziende e delle organizzazioni sulle quali è posta l'obbligazione di fornire la documentazione attestante la natura non "ad alto rischio" dei sistemi di IA, in base a meccanismi di puro *self-assesment*, sui quali viene "scaricata" ogni responsabilità. Impostazione che, se coerente rispetto alla scelta del legislatore dell'Unione di non includere il programmatore tra i soggetti

potenzialmente responsabili di violazioni di diritti fondamentali per opera di sistemi di IA, appare anch'essa criticabile tanto che oltreoceano è stato adottato un approccio diametralmente opposto (Cfr., la legge dello Stato del Colorado, c.d. CAIA).

In definitiva, urgente è l'intervento della Commissione, nella speranza che sarà all'altezza di un compito tanto arduo, ma altrettanto cruciale: emendare le rigidità, però fittizie, del Regolamento e chiarire che cosa *si può* e cosa *non si può* fare, facendo dell'intelligenza artificiale un'amica e non una nemica delle persone e dei loro diritti, come direbbe, forse, la nostra Corte costituzionale.

EDOARDO RAFFIOTTA

Uno dei settori su cui l'AI sta impattando maggiormente e – soprattutto – per i quali è possibile intravedere le maggiori possibilità di crescita è certamente quello del *fintech*.

Da un punto di vista generale, l'AI si candida al ruolo di prossimo fattore di rivoluzione del settore innanzitutto per la capacità di esaminare enormi moli di dati, automatizzare processi e ottimizzare le interazioni con i clienti (ad esempio attraverso chatbot, eventualmente anche personalizzati sulla base del profilo investitore). In tutto questo, certamente uno degli usi principali dell'AI nel *fintech* è rappresentato dalla valutazione del *credit-scoring*. Sempre più le istituzioni finanziarie sfruttano algoritmi di machine learning per misurare la solvibilità dei potenziali clienti con maggiore accuratezza rispetto ai metodi tradizionali: grazie a questi modelli è possibile ottenere una valutazione d'insieme della complessiva affidabilità creditizia del cliente impiegando in tale valutazione anche elementi oltre il punteggio di credito, come ad esempio i trascorsi finanziari, tipologia e frequenza dei movimenti bancari e finanziari, modelli di spesa, ecc. E, in definitiva, una migliore valutazione del merito creditizio favorirà entrambe le parti: da un lato permettendo ai clienti davvero meritevoli di ottenere il credito più facilmente (poiché ci sarà un maggiore margine di sicurezza della decisione), dall'altro migliorando la capacità delle istituzioni di contenere i tassi di insolvenza. Per tali ragioni, anche la prevenzione di frodi è una ulteriore ramificazione del settore fintech in cui l'AI avrà certamente un impatto estremamente significativo.

Ovviamente nessuna "opportunità" è esente da rischi. L'uso dell'AI nel settore *fintech*, e in particolare nel *credit scoring*, implica rischi e sfide che non possono essere ignorati.

L'uso dell'intelligenza artificiale (AI) nel settore fintech, e in particolare nel credit scoring, offre innumerevoli opportunità per migliorare l'efficienza e la precisione nel processo di concessione dei prestiti. Tuttavia, presenta anche una serie di rischi e sfide che devono essere affrontati per garantire che queste tecnologie siano utilizzate in modo responsabile e giusto.

Uno dei principali rischi associati all'uso dell'AI nel credit scoring è la possibilità di bias e discriminazione. Gli algoritmi di *machine learning* si basano sui dati storici per apprendere e fare previsioni, e se questi dati contengono pregiudizi o iniquità, c'è il

rischio che l'AI perpetui o addirittura amplifichi tali stati di fatto. Ad esempio, se i dati utilizzati per addestrare un modello di scoring includono informazioni che riflettono disuguaglianze socioeconomiche, l'algoritmo può finire per penalizzare ingiustamente determinate categorie di individui, come quelli appartenenti a minoranze etniche o a gruppi svantaggiati. Ciò non solo compromette l'equità nel processo di concessione dei prestiti, ma può anche generare conseguenze legali e reputazionali per le istituzioni finanziarie.

Inoltre, la mancanza di trasparenza nei modelli di AI rappresenta un altro rischio significativo. Molti algoritmi di *machine learning* operano come "scatole nere", rendendo difficile per le istituzioni e per gli utenti comprendere come vengono prese le decisioni. Questa opacità può ridurre la fiducia dei consumatori nei sistemi di scoring automatizzati e complicare i processi di audit e controllo. Se un cliente viene rifiutato per un prestito, avere la capacità di spiegare il motivo basandosi su criteri chiari e comprensibili è fondamentale sia per la soddisfazione del cliente che per la conformità alle normative.

Inoltre, l'affidabilità e la sicurezza dei dati utilizzati nell'AI sono di cruciale importanza. La raccolta e l'analisi di grandi volumi di dati sensibili, come le informazioni finanziarie personali, incrementano il rischio di violazioni della privacy e di attacchi informatici. Se i dati vengono esposti o manipolati, non solo la qualità del credit scoring può essere compromessa, ma gli individui possono anche subire danni significativi in termini di privacy e sicurezza.

Un altro aspetto da considerare è la dipendenza eccessiva dalla tecnologia. L'affidamento su sistemi di AI per decisioni critiche come *il credit scoring* può portare a una diminuzione del giudizio umano e a una scarsa considerazione per le circostanze individuali dei richiedenti. Ciò può comportare situazioni in cui l'AI non tiene conto di fattori specifici e contestualizzati che un operatore umano, in grado di valutare le sfumature delle esperienze individuali, potrebbe osservare.

Infine, l'evoluzione delle normative sul trattamento dei dati e sulla protezione dei consumatori può porre delle sfide per le istituzioni *fintech*. Le organizzazioni devono rimanere aggiornate sulle leggi in continua evoluzione riguardanti la privacy dei dati e l'uso dell'AI, e le violazioni possono comportare sanzioni significative. L'incertezza normativa può anche influenzare le decisioni aziendali e la progettazione dei modelli di scoring.

In sintesi, mentre l'AI ha il potenziale per trasformare il settore *fintech* e migliorare il *credit scoring*, è essenziale considerare e mitigare i rischi associati all'utilizzo di queste tecnologie. La necessità di garantire equità, trasparenza e sicurezza è fondamentale per costruire fiducia nei sistemi finanziari e massimizzare i benefici per tutti gli utenti.

Consideriamo ancora, ad esempio, la possibilità di bias e discriminazioni: sappiamo già che gli algoritmi possono diventare vittima delle loro stesse "banche dati": se i dati tramite i quali si alimentano contengono al proprio interno dei "bias" e delle c.d. discriminazioni algoritmiche, allora sappiamo che vi è il rischio che l'AI perpetui o addirittura amplifichi queste discriminazioni, creando un "circolo vizioso" nel quale le

previsioni e le convinzioni dell'AI si auto-avverano; andando in definitiva a ledere gli interessi fondamentali dei singoli.

Anche per tali ragioni è fondamentale allora costruire una AI che sia e possa dirsi *trustworthy*, capace di guadagnarsi la fiducia dei cittadini; e – al contempo – sarà pur sempre necessario affiancare all'impiego dell'AI la supervisione umana, capace di garantire un controllo accurato e di gestire accuratamente i sempre più complessi processi di compliance (*a fortiori* in un contesto, come si diceva, di progressivo aumento delle difficoltà interpretative della norma).

V Domanda

Guardando al contesto nazionale, ritiene che la nuova disciplina si ponga in continuità con la giurisprudenza amministrativa in tema di decisione automatizzata?

FRANCESCA BAILO

Com'è noto, la giurisprudenza amministrativa ha adottato un approccio particolarmente garantista a tutela del diritto di difesa dei cittadini, richiedendo una trasparenza algoritmica pressoché integrale (al proposito, *ex plurimis*, Cons. Stato, sez. VI, 8 aprile 2019, n. 8472, Tar Lazio, sez. III, 11 luglio 2018, n. 9230; Id., dec. 13 settembre 2019, n. 10963; decc. n. 9224-9230 del 2018; dec. 14 febbraio 2017, n. 3769, per le quali v. da ultimo la ricostruzione di M. FRANCAVIGLIA, *L'intelligenza artificiale nell'attività amministrativa: principî e garanzie costituzionali nel passaggio dalla regula agendi alla regola algoritmica*, in *Federalismi.it* n. 17/2024, 115 ss.). Secondo un orientamento ormai consolidato, occorre cioè poter conoscere sinanco il codice sorgente e, dunque, la formula tecnica dell'algoritmo, in modo tale che questa sia corredata da spiegazioni in grado di trasformarla in una regola giuridica comprensibile, nel rispetto della conoscibilità della motivazione che connota il provvedimento amministrativo. Allo stesso tempo, per superare il rischio che il diritto di accesso al ridetto codice sorgente risulti un mero "simulacro" formale, se ne rafforza la trasparenza, richiedendosi che la conoscibilità debba investire tutti gli elementi essenziali del sistema algoritmico utilizzato "dai suoi autori, al procedimento usato per la sua elaborazione, al meccanismo della decisione comprensivo delle priorità assegnate nella procedura di valutazione e decisionale dei dati selezionati come rilevanti" (v. Cons. Stato, sez. IV, dec. n. 8472/2019.).

Questa sorta di "legalità algoritmica", positivizzata da ultimo nell'art. 30 del d.lgs. 31 marzo 2023, n. 36 con specifico riferimento alla materia dei contratti pubblici, sino ad oggi è stata fondata anche sugli artt. 13, 14, 15 e 22 del GDPR (oltre al considerando n. 71), laddove, in riferimento a processi decisionali automatizzati, è previsto che il titolare del trattamento debba fornire "informazioni significative sulla logica utilizzata,

nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato" e che correlativamente, i destinatari possano accedere alle "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento".

Previsioni, queste ultime, che, tuttavia, andrebbero interpretate anche alla luce del considerando n. 63 che tutela i diritti di proprietà intellettuale, nella parte in cui chiarisce che il predetto diritto di accesso "non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software".

La spiegabilità astratta dell'algoritmo, negli intenti del legislatore eurounitario, non dovrebbe dunque squarciare il velo della *black-box* dell'algoritmo anche se poi, dall'art. 22 del GDPR, letto anche alla luce del considerando n. 71, sembrerebbe potersi desumere (sia pur con tutta una serie di eccezioni) una spiegabilità dell'algoritmo in concreto, *ex post*, da parte dell'interessato (oltreché dal giudice stesso). Si creerebbe, in buona sostanza, una sorta di apparente antinomia che però pare superata per il fatto che lo stesso considerando 63 specifica che il diritto di proprietà non dovrebbe "condurre a un diniego a fornire all'interessato tutte le informazioni", consentendo di modulare il diritto alla conoscibilità dell'algoritmo con il diritto di proprietà intellettuale.

Su un quadro normativo e giurisprudenziale, comunque, particolarmente complesso si innesta ora il regolamento sull'*AI Act* che, in specie all'art. 13, parrebbe, in genere, voler ancora maggiormente valorizzare il dovere di trasparenza circa la progettazione e il funzionamento dei sistemi di intelligenza artificiale. Con riferimento ai sistemi ad alto rischio, poi, lo stesso specifica che questi debbano essere progettati e sviluppati "in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'*output* del sistema e utilizzarlo adeguatamente" (art. 13.1).

Per comprendere se sul punto il regolamento fornisca una maggior tutela agli interessati e se si possa intravedere un cambio di paradigma (e, cioè, da un diritto di spiegabilità *ex ante* ad una spiegabilità anche *ex post* dell'algoritmo) tuttavia occorrerà, verosimilmente, attendere quale sarà l'indirizzo interpretativo che si consoliderà in ordine all'espressione "sufficientemente trasparente" (art. 13, par. 1 del regolamento).

Parimenti, per quel che concerne il principio di non esclusività algoritmica, il regolamento sembra ancor più rigoroso rispetto all'art. 22 del GDPR, dal momento che si richiede una sorveglianza umana non solo nella fase di progettazione e monitoraggio del sistema ma in ogni fase del funzionamento, consentendo all'utilizzatore di ottenere un controllo pieno della macchina e la possibilità di arrestarne il funzionamento. Novità, quest'ultima che, dovrebbe essere vista con favore e che, per non rimanere inattuata, comporterà l'esigenza che l'utilizzatore conosca a fondo il sistema in modo da poterlo integralmente gestire (in tal senso, cfr. anche l'art. 14 del regolamento, per i sistemi ad alto rischio), rafforzando, anche sotto questo profilo, il diritto alla trasparenza algoritmica.

Volendo però domandarsi se in detta disciplina vi sia una certa continuità tra quest'ultima e la giurisprudenza amministrativa e il legislatore nazionali può

condivisibilmente [v., in tal senso, G. LO SAPIO, *L'Artificial Intelligence Act e la prova di resistenza per la legalità algoritmica*, in *Federalismi.it*, n. 16/2024, 286] affermarsi, almeno a prima lettura, che il principio di trasparenza non è declinato allo stesso modo dal momento che la disciplina eurounitaria parrebbe pur sempre configurare una (più o meno) marcata asimmetria informativa a favore dei *provider*, dal momento che restano questi i detentori del potere di filtrare ciò che deve essere conoscibile dagli utilizzatori e da tutti gli altri soggetti della filiera, sicché "mentre nella prospettiva della tutela offerta sul piano giurisprudenziale e normativo interno, la trasparenza è il presupposto per riporre fiducia nelle decisioni algoritmiche; nel contesto dell*'IA Act*, la trasparenza elargita dai provider presuppone che vi sia a monte fiducia da parte degli utenti finali che essi effettivamente mettano a disposizione le informazioni utili per conoscere e comprendere i sistemi immessi sul mercato". Ciò con l'effetto, già sottolineato da attenta dottrina [A. DI MARTINO, *Tecnica e potere nell'amministrazione per algoritmi*, Napoli, 2023, 194], secondo cui parlare «di trasparenza potrebbe quindi risultare fuorviante", emergendo "un ennesimo momento di tensione tra la funzione ordinatrice e di garanzia del diritto e il ruolo ancillare della tecnica, arricchita dalla oscurità intrinseca che riguarda non solo l'algoritmo, ma, più in generale, la traiettoria di sviluppo delle decisioni pubbliche che hanno traghettato i pubblici poteri in una *black box society*". Nella prospettiva eurounitaria sembrerebbe, cioè, essere imposto un obbligo di trasparenza che, nella pragmatica consapevolezza della complessità e oscurità dell'algoritmo, si risolve in una serie di obblighi di informazione per i *provider* in modo tale che vi sia una trasparenza sufficiente e adeguata ma che rimanga pure sempre nella loro discrezionalità e competenza tecnica. Il che depotenzia, in certa misura la previsione del diritto alla spiegazione di cui all'art. 86 del regolamento che pure parrebbe riguardare un controllo *ex post* della singola decisione.

GIOVANNA DE MINICO

In premessa è utile evidenziare che dall'art. 97 Cost. discende direttamente il dovere di trasparenza, che impone all'amministrazione la visibilità dei suoi percorsi decisionali. Ogni potere pubblico, non solo quello rappresentativo, dev'essere al servizio della volontà dei cittadini; di conseguenza, per obbedire a questo vincolo funzionale, il potere deve restare sempre in bella vista, così da sottoporsi al continuo controllo dei cittadini.

Come si garantisce tale risultato quando nel procedimento amministrativo entra l'IA?

Il diritto alla motivazione algoritmica può essere una via quando il processo decisionale da monocratico e autoritario di fatto si è convertito in "misto" per la compresenza delle volontà umana e meccanica. Se l'autorità pubblica utilizza algoritmi, questa delega di funzionamento alla macchina non dovrebbe diventare un facile alibi per una reintroduzione dell'oscurità autoritativa. Nel caso in cui l'atto accetti gli esiti algoritmici, non basterà una motivazione *per relationem*, altrimenti cadremmo in un

ragionamento tautologico, in quanto tale oscuro. Sarebbe come dire: l'amministrazione ha deciso così, perché così vuole l'algoritmo. Al contrario, l'autorità pubblica sarà tenuta a spiegare in termini chiari e comprensibili perché ha accettato il risultato della macchina, dal momento che l'algoritmo è chiuso in se stesso e non dice nulla sulle ragioni del suo funzionamento. Nel caso contrario, ovvero se l'amministrazione si discostasse dai risultati algoritmici, dovrà fornire motivazioni esplicite, come avverrebbe nel caso in cui l'autorità pubblica disattendesse un parere obbligatorio precedentemente richiesto. Le caratteristiche inerenti alla trasparenza dell'atto algoritmico, a partire dalla sentenza del Cons. Stato, Sez. VI, 2019, n. 2270, "concorrono a definire il contenuto della motivazione del provvedimento" [L. GRIMALDI, *Costituzionalismo «post-umano» alla prova della decisione pubblica algoritmica*, in *Federalismi.it*, 34/2022, 89]

Quanto al rapporto tra *AI Act* e Regolamento n. 679/2017 (d'ora in poi *GDPR*), mi pare si possa affermare l'esistenza di un rapporto di specialità tra gli stessi, come afferma l'art. 2, par. 7 dell'*AI Act*.

La continuità tra i medesimi inizia a incrinarsi sotto il profilo della loro *governance*: si designano distinte autorità per la vigilanza dei due mercati, peraltro non equivalenti sul piano dell'indipendenza e dell'autonomia dal potere. Mentre il Garante nazionale della protezione dei dati personali presenta tutte le caratteristiche di un'autorità amministrativa indipendente, l'autorità garante dell'IA non è geneticamente indipendente dal Governo e per un'illustrazione approfondita di questo vizio o virtù rinvio alla risposta della domanda 6.

Guardando al catalogo dei diritti dei due Regolamenti da un lato l'art. 86 dell'AI Act riconosce alla persona il diritto di ricevere dal *deployer* le ragioni per cui ha ricevuto una data decisione dalla macchina; dell'altro, l'art. 22 del GDPR riconosce alla persona il diritto a ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione meccanica.

In breve, l'*AI Act* offre un catalogo frammentato dei diritti (artt. 13, 50 e 86), da cui si possono comunque ricavare tre attributi qualificatori la trasparenza, a differenza di una visione di insieme dei diritti fondamentali contenuta nel GDPR.

1) La trasparenza come mezzo per la piena conoscibilità dell'atto algoritmico.

2) La trasparenza che cambia al mutare della tecnologia.

3) La trasparenza che cambia al mutare delle finalità dell'atto.

Questi tre momenti devono convertire la segretezza automatizzata in visibilità. Il fine della *disclousure* è la misura di effettività dell'equazione: conoscibilità dell'atto/sua sfidabilità in giudizio (art. 113 Cost. impugnabilità che non conosce eccezioni). Ciò significa che l'informazione deve garantire una comprensione effettiva del *reasoning* meccanico e, dunque, comporsi degli *input* inseriti, del punteggio di ciascuno, dei rispettivi criteri di valutazione e, infine, della logica intrinseca di funzionamento.

L'*AI Act* fa un passo avanti rispetto al *GDPR* poiché prevede la motivazione, non solo come elemento essenziale del provvedimento, ma come pretesa dell'individuo a una spiegazione minima e comprensibile [G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, 2/2024, 88 ss.]. Tuttavia, quale è il

punto limite, oltre il quale il diritto di essere informati non può andare? Il diritto alla *disclousure* prevale sul segreto industriale fino a coinvolgere il codice sorgente oppure è predicabile l'inverso?

La questione non è nuova, era stata già affrontata dal *GDPR*, che nel *Considerandum* 63 spiegava che il segreto commerciale non giustificava il rifiuto assoluto a ogni informazione sugli algoritmi; dall'altro canto, il diritto alla divulgazione non poteva spacchettare il codice sorgente, ma si doveva arrestare alle caratteristiche e alla logica specifica degli algoritmi utilizzati. Nello scontro tra la *privacy* e i diritti antagonisti il *GDPR* non accordava una superiorità astratta ed *ex ante* al primo a discapito delle altre situazioni soggettive [G. MALGIERI, G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 3/2017; M.E. KAMINSKI, *The right to explanation, explained*, in *Berkeley Tech Law Journal*, 34/2019]. Nella *querelle* sul bilanciamento, il *GDPR*, obbedendo al principio di proporzionalità, assicura il diritto di accesso alla logica algoritmica nella misura massima possibile, non fissata in un'entità immodificabile, ma modulabile all'occorrenza, in ragione dell'identità del richiedente la spiegazione.

L'*AI Act* conferma la scelta di non introdurre un diritto assoluto alla *meaningful information*, riconoscendo il diritto alla motivazione a condizione che non leda i controdiritti, come previsti da altra normativa europea. A differenza però del *GDPR*, non si fa menzione dei controdiritti, ma si preferisce la tecnica del rinvio.

A incrinare le luci del catalogo dei diritti sull'IA è l'ombra della *black box* [F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge-London, 2015]. Al diritto alla spiegazione significativa corrisponde forse un divieto all'utilizzo di IA irrimediabilmente opache? Mi sto chiedendo se l'IA possa procedere al di fuori della giurisdizione di chi l'ha istruita e disegnata, non per ragioni di difesa del *trademark*, ma perché l'autoaddestramento e l'autogenerazione del codice della macchina rendono ignoto il suo effettivo funzionamento. Qui si crea una catena di ignoranza tra fornitore, utente commerciale e utente finale, che attende nuove pronunce giurisprudenziali.

EDOARDO RAFFIOTTA

La giurisprudenza amministrativa ha preso una posizione netta sul tema dell'impiego dell'AI a partire dalle note decisioni del TAR Lazio nn. 9924/2018 e 6606/2019, il cui orientamento è stato poi recentemente ribadito da TAR Lazio n. 10964/2022: in estrema sintesi, come noto agli addetti ai lavori, il principio di diritto cui la giurisprudenza amministrativa si conforma è quello per cui "Le procedure informatiche finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, *non possono mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere* e che pertanto, al fine di assicurare

l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il *dominus* del procedimento stesso" (sottolineato aggiunto).

L'*AI Act*, allora, può ben dirsi – almeno su questo punto – in linea con la giurisprudenza amministrativa italiana, il cui cardine è l'imprescindibilità del giudizio umano nei processi decisionali. Entrambi condividono una visione per cui, nonostante i progressi tecnologici, le macchine non possono interamente rimpiazzare la valutazione e il discernimento umano, specialmente in contesti che coinvolgono diritti e interessi individuali.

Non è un caso che tutte le decisioni che impattano in maniera fondamentale sulla vita dell'individuo prevedano alcuni baluardi di sicurezza, tra cui l'impiego di una intelligenza artificiale che sia trasparente, tracciabile e, soprattutto, soggetta al controllo umano.

Analogamente, non possiamo dimenticare la n. 2270/2019 del Consiglio di Stato (c.d. caso della "buona Scuola"), che ha ben chiarito che se "l'algoritmo, ossia il *software*, deve essere considerato a tutti gli effetti come un atto amministrativo informatico", allora deve sottostare alla relativa disciplina, stante il principio per cui "l'utilizzo di procedure "robotizzate" non può essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa". Ne deriva allora "che il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere "conoscibile", secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico". Inoltre, e soprattutto – e qui è evidente il *fil rouge* con quanto si diceva sopra – "la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo": e questo poiché "solo in questo modo è possibile svolgere, anche in sede giurisdizionale, una valutazione piena della legittimità della decisione; valutazione che, anche se si è al cospetto di una scelta assunta attraverso una procedura informatica, non può che essere effettiva e di portata analoga a quella che il giudice esercita sull'esercizio del potere con modalità tradizionali".

In conclusione, è innegabilmente positivo lo spirito dell'*AI Act* nella parte in cui si pone come strumento per disciplinare l'impiego dell'intelligenza artificiale in modo che rispecchi i valori fondamentali dell'interazione umana e sia in grado di amalgamare quest'ultima e la pubblica amministrazione.

VI Domanda

In una prospettiva *de iure condendo*, come valuta la proposta di legge A.S. 1146 (XIX legislatura) "Disposizioni e delega al Governo in materia di intelligenza artificiale"?

FRANCESCA BAILO

La proposta di legge, di iniziativa governativa, è stata comunicata alla Presidenza del Senato il 20 maggio 2024 esattamente un giorno prima della definitiva approvazione del regolamento sull'intelligenza artificiale da parte del Consiglio dell'Unione europea e, dunque, il nostro è il primo Stato membro a fornire una disciplina nazionale che vada ad integrare e/o normare la materia negli ambiti in cui il Regolamento ha lasciato che fossero i legislatori nazionali ad intervenire, pur dovendo questi legiferare in modo conforme al diritto eurounitario.

Essa si propone, dunque, di operare un bilanciamento tra opportunità e rischi dell'impiego dell'intelligenza artificiale non già sovrapponendosi alla normativa europea ma, semmai, "accompagnandola", col promuovere una gestione del rischio fondata su una visione antropocentrica e, al contempo, disporre norme di principio e disposizioni di settore atte a far sì che le nuove tecnologie vadano a migliorare la vita dei cittadini e la coesione sociale nel rispetto e a tutela dei diritti fondamentali, la democrazia, lo Stato di diritto e la sostenibilità ambientale.

Tra le norme che suscitano particolare interesse, si segnala l'art. 22, commi 1, 2 e 6, che delega il Governo ad adottare, entro dodici mesi dall'entrata in vigore del provvedimento, uno o più decreti legislativi per adeguare la normativa nazionale al regolamento medesimo, ai sensi dell'art. 31 della l. n. 234/2012, il quale prevede l'acquisizione del parere – oltre che delle Commissioni parlamentari competenti – del Garante per la protezione dei dati personali. Tra i principi e criteri direttivi detto articolo stabilisce, altresì, che il Governo designi l'autorità di vigilanza del mercato, l'autorità di notifica, nonché il punto di contatto con le istituzioni dell'Unione europea, in coerenza con l'art. 18 che, ad integrazione di quanto richiesto dal regolamento europeo, qualifica quale Autorità nazionali per l'intelligenza artificiale due soggetti e, cioè, l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale, oltre a un Comitato di coordinamento presso la Presidenza del Consiglio per agevolare la collaborazione delle due Agenzie tra loro e con le pubbliche amministrazioni. Questo modello di *governance*, tuttavia, non convince del tutto dal momento che, come rilevato dal Garante per la protezione dei dati personali, occorrerebbe un maggior coinvolgimento della medesima autorità, esemplarmente, nell'istituendo Comitato, o laddove non è previsto che AgID e ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati.

L'articolo 22, commi da 3 a 5, delega poi il Governo, a dare una definizione organica della disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite, sì da completare idealmente quanto statuito all'art. 25, il quale introduce una fattispecie di reato, una circostanza aggravante comune e limitate circostanze aggravanti ad effetto speciale per alcuni reati. Tuttavia, sembrerebbe che detta delega, che, tra l'altro, prevede anche l'introduzione di una o più autonome fattispecie di reato incentrate sull'omessa adozione o l'omesso adeguamento di misure di sicurezza per la

produzione, la messa in circolazione e l'utilizzo professionale di sistemi di intelligenza artificiale, o dirette a tutelare specifici beni giuridici esposti a rischio di compromissione per effetto dell'utilizzazione di sistemi di intelligenza artificiale, appaia forse eccessivamente ampia.

Di specifico interesse è, infine, l'art. 14 del testo che, nel disciplinare l'uso dell'intelligenza artificiale nell'attività giudiziaria, ne restringe il campo esclusivamente all'organizzazione e alla semplificazione del lavoro giudiziario, nonché alla ricerca giurisprudenziale e dottrinale specificandosi unicamente, al comma 2, che è sempre riservata al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento.

GIOVANNA DE MINICO

Il disegno di legge italiano sull'IA risolve i suoi pregi nella fedeltà piena al Regolamento n. 1689/2024. Tuttavia, questa positività è anche il suo vizio perché persino dove avrebbe potuto derogare all'*AI Act* senza incorrere in un'illegittimità comunitaria si è conformato al primo.

Il caso emblematico è rappresentato dalla *governance.* Per meglio comprendere la situazione è necessario fare un passo indietro: l'autorità nazionale di vigilanza nella versione iniziale - intendo quella consegnata nell'art. 59 e succ. emendamenti del Parlamento europeo, 14 giugno 2023 - era "organizzata e gestita in modo tale da salvaguardare l'obiettività e l'imparzialità dei suoi compiti e delle sue attività". Dunque, il suo disegno era stato tracciato in coerenza col principio di separazione della politica dall'amministrazione. Infatti, le autorità nazionali, individuabili da ciascuno Stato in autonomia, avrebbero dovuto obbedire a un unico precetto: mantenersi indipendenti geneticamente e poi funzionalmente dagli Esecutivi nazionali. Il dato normativo, l'art. 59, co. 4 bis, disponeva che: "Ciascuna autorità nazionale di controllo esercita i propri poteri e svolge le proprie funzioni in modo indipendente, imparziale e senza pregiudizi. Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, i membri di ciascuna autorità nazionale di controllo non sollecitano né accettano istruzioni da alcun organismo e si astengono da qualsiasi atto incompatibile con il carattere delle loro funzioni".

Il testo dell'*AI Act* ha subito significativi emendamenti in sede di trilogo tanto che alcune delle sue parti sono così distanti dalla matrice originaria da essere irriconoscibili. Questa nuova veste è dovuta alle pressioni esercitate da alcuni Stati, che hanno determinato un'inversione a U della *governance* nazionale con il risultato di affidare all'autonomia domestica di ciascuno Stato, non solo la scelta delle autorità, ma anche il metodo per la loro designazione: come collocarle all'interno dell'ordine giuridico statale. Così l'attuale art. 70 dell'*AI Act* ha aperto la via all'opzione governativa italiana. Quest'ultima si è risolta – d.d.l. A.S. 1146 *Disposizioni e delega al Governo in materia di intelligenza artificiale* all'art. 18 – nell'investitura di due agenzie governative preesistenti: l'Agenzia per l'Italia digitale e l'Autorità di cybersicurezza nazionale.

Invero, il Garante della privacy il 25 marzo 2024 già aveva segnalato al Parlamento e al Governo il rischio di disallineamento tra *AI Act* e *GDPR*, indicando validi motivi a sostegno della tesi di mantenere anche i compiti inerenti all'I.A. all'Autorità già deputata alla protezione della nostra privacy e al controllo dell'integrità e inviolabilità del flusso dei dati. Tra questi argomenti hanno attirato la mia riflessione i seguenti: 1) la sua vantata indipendenza dall'Esecutivo; 2) l'utilità di non duplicare le autorità, stante la preesistenza di quella sui dati, mentre un raddoppio avrebbe condotto a possibili "giudicati" antagonisti; 3) la designazione del Garante per la protezione dei dati da parte dell'*AI Act* nei settori individuati nell'All. III, a testimonianza del *favor* europeo per questa soluzione organizzativa.

Nonostante le ragionevoli ragioni a sostengo dell'istanza del Garante, il d.d.l. ha scelto soggetti antitetici al modello autorità indipendente nel momento in cui ha rispolverato la comitologia comunitaria, la cui provvista è rimessa appunto alla disponibilità della maggioranza di Governo. Se è vero che la larghezza del tessuto normativo, propria del Regolamento, non obbligava gli Stati, e quindi neppure l'Italia, a scegliere il modello dell'autorità insensibile al comando politico di maggioranza, è pur vero che la medesima elasticità non le imponeva l'idealtipo opposto.

Il moto centripeto della *governance* ha avuto un'accelerazione con il nostro d.d.l., che infatti - l'art. 17 - assegna alla Presidenza del Consiglio dei Ministri il compito di elaborare la strategia nazionale di IA con l'aiuto di Agid e Acn. Sono evidenti le ragioni di questa scelta: visto che l'intelligenza meccanica si candida a essere lo strumento essenziale per le *policy* pubbliche, sarà irrinunciabile tanto per l'azione preventivo-punitiva che per quella occupazionale o per il controllo dei flussi migratori alle frontiere, beninteso si tratta di esiti ancora al di là da venire, ma che sono già sullo sfondo. Pertanto, il Governo ha opportunamente pensato di acquisire la mente meccanica da subito a sé piuttosto che affidarla con una delega in bianco ad Autorità estranee alla sua giurisdizione politica, quale dovrebbero essere le autorità indipendenti, almeno quelle rientranti nel paradigma istituzionale in deroga all'art. 95 Cost. Allora, se la volontà del decisore politico è di mantenere strette nelle sue mani le chiavi per aprire e chiudere il flusso dei bit intelligenti, è scontata l'opzione per il modello comitologia, che lascia le Autorità un passo indietro rispetto al Governo e comunque le pone sotto la sua ala protettiva. Non va però dimenticato che se si tratta di un modello coerente con l'indirizzo politico di maggioranza, questo attributo è al tempo stesso anche il suo punto di debolezza perché sarà causa di un'intelligenza fisiologicamente asservita al mutevole orientamento delle famiglie politiche, inevitabilmente ancillare ai valori politici contingenti, e disinvolta rispetto a quel *common good,* individuato una volta per tutte dal Regolamento e orientato alla visione umano-centrica della nuova tecnica.

Se invece si ritiene che i settori sensibili debbano essere tenuti indenni dalle direttive della maggioranza di turno, il che da un punto di vista concettuale significa accostare questi settori a valori di rango costituzionale, meritevoli di tutela continuativa e nella misura massima possibile, le Autorità che presiedono l'Intelligenza andranno isolate dalla politica, collocate in un'area intoccabile dall'indirizzo politico-rappresentativo, con il pericolo che l'intelligenza da assistente del Governo slitterà alle

dipendenze delle Autorità indipendenti. E qui si riproporrà la domanda di sempre: chi risponderà delle scelte di una mente meccanica al servizio di Autorità, a loro volta politicamente irresponsabili?

In antitesi a questa visione c'è chi non apprezza le autorità indipendenti perché poco o troppo autonome dai vertici politici, e pertanto condividerà la scelta del nostro Governo, che ha almeno il pregio di fare salva una regola fondamentale della democrazia: chi assume decisioni politiche ne deve rispondere politicamente.

Tuttavia, non si può tacere che il rischio della cattura sia dietro l'angolo. Le autorità di vigilanza attiveranno i loro poteri di indagine nei confronti di una PA o di un'impresa che si muove in linea con la Strategia nazionale, ma in violazione del Regolamento europeo?

Ma a un'osservazione più attenta il rischio della cattura si presenta addirittura tridirezionale perché l'autorità di vigilanza potrebbe essere catturata dall'IA stessa in quanto è poco credibile che il soggetto pubblico, autore dell'atto amministrativo intelligente, abbia conservato un'effettiva autonomia decisionale rispetto all'*output* della macchina, come dicono i francesi, preoccupati dall'*effet moutonnier*. Il pericolo per l'autorità decidente è rimanere vittima dell'influenza della macchina, dalla quale si sottrarrà solo con un *surplus* di istruttoria e di autonomia decisionale, cioè facendo semplicemente il proprio lavoro. Ma quale funzionario pubblico, amministratore o giudice, sarà disposto a rifare la laboriosa attività della macchina pur di dire la sua? Questo *nudge* sulla discrezionalità del soggetto pubblico non è mitigato dal sistema di supervisione in esame, neppure se esso in un sussulto di fantasia giuridica istituisse un giudice speciale europeo, ex art. 263, co. 5, TFUE [G. DE MINICO, *Internet e le sue regole*, in M. CALAMO SPECCHIA (a cura di), *Processi politici e nuove tecnologie*, cit.], tralasciando le obiezioni istituzionali che tale figura atipica solleverebbe, a mio avviso superabili.

Infine, come l'*AI Act*, anche il d.d.l. 1146, art. 18, co. 2, non chiarisce la regola procedurale da adottare nel caso in cui una misura correttiva di un'Autorità invadesse l'area di competenza dell'altra. L'istituzione di un Comitato di coordinamento per il raccordo con le altre autorità indipendenti e PA, assegna ad Agid e Acn il compito di collaborare, ma non è detto a chi spetti la parola definitiva.

Con questa ultima domanda voglio solo dire che rispolverare l'antico istituto della comitologia crea più problemi di quelli che vorrebbe risolvere, non ultimo il contrasto tra giudicati, anche se impropriamente detti, pronunciati da Autorità diverse in natura e poco inclini al dialogo reciproco.

Mi scuso con la mia lettrice/lettore se alle domande che la Redazione ha ragionevolmente formulato non sempre ho risposto con pensieri definitivi, offrendo invece avvii per una nuova riflessione e per ulteriori domande che a mia volta rivolgo a chi avrà la pazienza di leggermi.

COSTANZA NARDOCCI

Nel quadro di quello che per lungo tempo poteva definirsi come un atteggiamento "attendista" degli Stati membri di fronte alle iniziative adottate a livello di Unione Europea, l'Italia ha occupato di recente una posizione di primo piano quale primo Stato membro a predisporre una proposta di legge in materia di intelligenza artificiale a distanza di pochi mesi dalla approvazione dell'*AI Act* del marzo 2024 (Interessante anche il caso della Spagna che, prima tra gli Stati membri, ha istituito un organismo di supervisione dei sistemi di IA: la *Agency for the Supervision of Artificial Intelligence*, AESIA).

L'accelerazione impressa dal Governo italiano non sorprende fino in fondo.

Vale, in proposito, ricordare il *Joint Paper*, sottoscritto nell'autunno del 2023 da Italia, Francia e Germania, volto a segnalare l'urgenza di introdurre una regolamentazione dell'impiego dei sistemi di IA anche oltre i recinti entro cui si stava all'epoca muovendo il dibattito in seno alle istituzioni euro-unitarie.

Il precedente esprime, quindi, una certa impazienza dell'ordinamento giuridico italiano, peraltro non isolata, e contestualmente la volontà di intervenire nella fase di concretizzazione della attesa disciplina dell'Unione.

La proposta di legge, attualmente in discussione, sicuramente presenta alcuni profili di interesse che meritano di essere presi in considerazione, soprattutto nella misura in cui segnalano un allentamento dal seminato dell'*AI Act.*

Avvicinandosi ad una impostazione più diffusa oltreoceano, il disegno di legge di iniziativa governativa fa propria una impostazione "settoriale", come si evince in modo esplicito dal Capo II, rubricato "Disposizioni di settore". Si preoccupa, cioè, di introdurre alcune norme di base, che si differenziano in ragione dell'ambito di impiego dei sistemi di intelligenza artificiale.

La scelta costituisce una prima differenza rispetto all'*AI Act* che, come già rilevato, offre una regolamentazione ad ampio spettro, allentando il collegamento, talvolta però di necessaria istituzione, tra tecnologie di intelligenza artificiale e settore di loro impiego. Da questo punto di vista, il disegno di legge si focalizza, tra gli altri, sul settore della sanità e su quello lavoristico.

Con riferimento a questi due ambiti, si scorgono alcune deviazioni rispetto alla disciplina europea, che sembrano indirizzate verso una maggiore cautela o irrigidimento nel ricorso agli strumenti di IA.

Per quanto attiene alle implicazioni delle tecnologie di intelligenza artificiale in ambito sanitario e di disabilità, a differenza dell'*AI Act*, il disegno di legge prevede, così, controlli aggiuntivi e più stringenti in tema di trattamento dei dati (Cfr. art. 8, comma 3).

Nel settore lavoristico, anche il disegno di legge proibisce ogni applicazione di sistemi di IA, che si riveli discriminatoria su base etnica, di genere, età, orientamento sessuale. Il disegno di legge va, però, oltre le affermazioni di principio e istituisce l'*Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro*, presso il Ministro del Lavoro e delle Politiche Sociali "con il compito di definire una

strategia sull'utilizzo dell'intelligenza artificiale in ambito lavorativo, monitorare l'impatto sul mercato del lavoro, identificare i settori lavorativi maggiormente interessati dall'avvento dell'intelligenza artificiale" (Cfr. art. 11).

Altrettanto interessanti sono le disposizioni dedicate alle modifiche del codice penale. L'intervento legislativo segue coerentemente la *ratio* dichiarata nella Relazione illustrativa di consentire l'attuazione del Regolamento EU entro l'ordinamento giuridico e introduce nuove circostanze aggravanti e anche nuove fattispecie incriminatrici. Pure rendendosi probabilmente opportuno un adattamento del quadro normativo, la circostanza che tali norme facciano perno sulla nozione di intelligenza artificiale, controversa, ereditata dall'*AI Act* potrebbe porsi alla base di criticità serie in punto di determinatezza e, in estrema sintesi, di rispetto del principio di legalità in materia penale.

Oltre l'impostazione, come detto, "settoriale", vi sono almeno altre due scelte del disegno di legge governativo, che meritano di essere richiamate in questa sede.

La prima è la istituzione di due organismi indipendenti preposti a presidiare l'utilizzo e le ricadute pubbliche e private dell'IA: l'AgID (Agenzia per l'Italia Digitale) ai sensi dell'art. 18 e l'ACN (Agenzia Nazionale di Cybersecurity) *ex* art. 6.

Meritoria è sicuramente la volontà di rafforzare il collegamento tra *cyber*sicurezza e mondo dell'intelligenza artificiale che, viceversa, a livello sovranazionale si fatica a ricondurre ad unità. Così accade, incidentalmente, tanto per l'Unione Europea quanto per il Consiglio d'Europa, dove la nuova Convenzione Quadro appare poco in raccordo con il previgente trattato in materia di sicurezza *cyber* e *cybercrime*, la c.d. Convenzione di Budapest.

L'opzione vagliata nel disegno di legge non è stata, però, accolta con favore dall'Autorità Garante per la Privacy, che ha rivendicato la propria competenza in materia e la necessità di attrarre a sé la vigilanza anche sull'impiego delle tecnologie di IA. Sul punto, non può sottacersi l'importante ruolo suppletivo assolto dall'Autorità negli anni che hanno preceduto l'approvazione dell'*AI Act*, le cui ordinanze di ingiunzione hanno sopperito alla inattività dell'autorità giudiziaria ponendo l'accento sulla esigenza imprescindibile di coniugare le tecnologie di IA con i principi costituzionali (Cfr. le ordinanze di ingiunzione del Garante del 10 giugno 2021 e del 22 luglio 2021, relative alle ricadute discriminatorie dei sistemi automatizzati di prenotazione delle sessioni di lavoro dei *riders*, gestite tramite l'impiego di sistemi algoritmici di *Glovo App23* e *Deliveroo s.r.l.*).

Un secondo elemento è dato, poi, dal riferimento più esplicito ed immediato al rispetto dei principi fondamentali e di non discriminazione, sebbene il risultato molto probabilmente risenti dell'intenso dibattito, promosso a più riprese da associazioni non governative, che avevano lamentano la scarsa sensibilità soprattutto della prima bozza dell'*AI Act* rispetto alla salvaguardia dei diritti fondamentali.

Accanto a quanto precede e nella impossibilità di prevedere i tempi e gli esiti del dibattito parlamentare, resta certamente da sottolineare l'opportunità che il disegno di legge si mantenga entro i binari della normativa euro-unitaria, che, allo stato, si trova ancora incompiuto sino alle linee guida di prossima adozione della Commissione.

Resta sullo sfondo del disegno di legge italiano, come già dell'*AI Act*, il tema della traduzione concreta delle norme di legge. Aspetto, forse, secondario per il disegno di legge governativo data la natura direttamente applicabile del Regolamento alle cui scelte il disegno di legge non potrà se non piegarsi e che, tuttavia e come già rilevato più volte, appare sul punto in parte carente. Occorrerà attendere l'intervento della Commissione e studiare come il disegno di legge si raccorderà con le sue linee di indirizzo. Una serie di interrogativi, che sollevano più di un dubbio sulla opportunità in termini di contenuti e di tempi di un intervento legislativo, quale quello promosso dal Governo italiano, che si inserisce in un frangente temporale in cui ancora troppo incerte sono le sorti della regolamentazione europea dell'intelligenza artificiale.

In chiusura, un ultimo aspetto riguarda le posizioni che assumeranno, *se* ne assumeranno, gli altri Stati membri dell'Unione Europea nelle more dell'intervento della Commissione. Ci si chiede, così: se seguiranno l'esempio italiano; se opteranno per regolamentazioni di dettaglio, nel tentativo di colmare le lacune del Regolamento ed anticipando la Commissione; se decideranno, all'opposto, di attendere le linee guida della Commissione, demandando ad organismi terzi ed indipendenti la gestione della eventuali ma probabili criticità scaturenti dal funzionamento dei sistemi di IA.

A prescindere dall'estrema varietà di ipotesi, a cui solo sommariamente si è accennato in questa sede, resta sullo sfondo il pericolo di una frammentazione tra le soluzioni vagliate a livello nazionale secondo una tendenza alla localizzazione, che contraddice l'atteggiamento, viceversa favorevole a riconoscere la precedenza e lo spazio del legislatore dell'Unione che ha caratterizzato, sino ad ora e in modo sintonico, l'*agere* degli Stati membri e di cui si dava conto in apertura di queste brevi riflessioni.

EDOARDO RAFFIOTTA

L'attuale governo sta dimostrando di aver adottato un approccio proattivo nella regolamentazione del digitale. L'obiettivo è chiaro: regolamentare i nuovi fenomeni digitali europei e, così facendo, affermarsi come interlocutori privilegiati del legislatore europeo.

Nel merito del ddl, sarà importante far convivere due anime della regolazione: da un lato la "vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale" (come non a caso indicato dall'art. 1 del testo normativo), dall'altro la necessità di aumentare gli investimenti nei settori dell'intelligenza artificiale e della cybersicurezza: in questo senso, se è vero che ci stiamo muovendo, è altrettanto vero che l'Italia (come anche l'Europa, del resto) non investe abbastanza e – quando lo fa – è troppo spesso prigioniera di lungaggini burocratiche e formalismi documentali. Occorre invece investire di più e meglio (dunque, più rapidamente e più efficacemente). Le strade da percorrere allora sono due: maggiori risorse per la ricerca e la sperimentazione (nel solco di quello che infatti promuove l'*AI Act* con gli spazi di sperimentazione normativa) e più spazio per regole di *soft law* e linee guida, anche da parte dei maggiori addetti ai lavori (tra cui AGID, ACN, Università e aziende).

ANDREA SIMONCINI

Sul disegno di legge AS 1146 "Disposizioni e delega al Governo in materia di intelligenza artificiale" mi sembra di poter esprimere tre valutazioni di fondo, quantomeno con riferimento versione ad oggi disponibile, sapendo che il percorso parlamentare non è ancora terminato.

La prima considerazione è l'apprezzamento per la scelta dello strumento del disegno di legge. In un'epoca di "emergenza infinita", in cui il decreto-legge è diventata la forma ordinaria di esercizio dell'iniziativa legislativa del governo, la scelta "controcorrente" di seguire il percorso fisiologico del disegno di legge e di attendere, dunque, la relativa discussione parlamentare mi pare molto importante. Soprattutto, la decisione di avviare l'iter parlamentare e non di anticipare la disciplina attraverso la decretazione d'urgenza, mi pare si imponga proprio per il contenuto proprio di questa proposta legislativa, che tocca una serie di problematiche molto delicate, che spaziano dai diritti fondamentali della persona, alla separazione dei poteri, alla sicurezza nazionale.

In secondo luogo, mi pare in altrettanto positivo il giudizio sulla parte del disegno di legge dedicata alla definizione dei principi generali in materia di IA, all'applicazione di tali principi ad alcuni settori sensibili ed alla delega al Governo per l'attuazione del Regolamento europeo AI act.

Il disegno di legge si pone in chiara continuità con l'impostazione del Regolamento Europeo ed intende "*promuove(re) un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale*."

Ad esempio, l'art. 3, secondo comma, del disegno di legge ripropone espressamente il principio per cui "*lo sviluppo di sistemi e di modelli di intelligenza artificiale avviene su dati e tramite processi di cui deve essere garantita e vigilata la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati*", ribadendo così quella fondamentale novità contenuta nell'art., 10 dell'AI Act su cui mi sono già soffermato.

D'altra parte, si afferma - all'art. 5 - che lo Stato ha un interesse alla promozione dell'utilizzo dell'IA come strumento per migliorare la produttività in tutte le catene del valore, così come la creazione di un mercato dell'IA "innovativo, equo, aperto e concorrenziale"; si ripropongono, quindi anche a livello nazionale i due obiettivi "gemelli" di protezione dei diritti e promozione della crescita economica.

L'impressione è che, quantomeno in alcune disposizioni, la definizione dei principi nella proposta di legge nazionale sia anche più completa e sistematica rispetto al Regolamento Europeo.

Altrettanto importanti sono il Capo II e il IV, in cui gli stessi principi generali vengono declinati all'interno di alcune aree particolarmente sensibili (salute, lavoro e

professioni, pubblica amministrazione, giustizia, cybersicurezza, diritto di autore e informazione).

Il punto, in realtà, che ha suscitato maggiori discussioni e che probabilmente merita una riflessione più approfondita, è il Capo III dedicato alla strategia nazionale alle autorità nazionali e alle azioni di promozione.

L'articolo 18 del disegno di legge sceglie di indicare come autorità nazionali incaricate di "garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale", l'Agenzia per l'Italia digitale (AGID) e l'Agenzia per la cybersicurezza nazionale (ACN).

Innanzitutto, va detto che la scelta è certamente consentita dal testo del Regolamento europeo che all'art. 70 chiarisce che "*ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro*"

Dunque, sul piano quantitativo le autorità possono essere "una o più". Ovviamente il fatto che *possono* non implica che *debbano* essere più di una. Si pone quindi l'interrogativo su quali siano le ragioni che hanno spinto il governo a questa duplicità, a fronte di alcune considerazioni problematiche quali, ad esempio, la distribuzione dei compiti tra i due soggetti. Il disegno di legge, sul piano della formulazione delle attribuzioni sembra essere abbastanza chiaro: da un lato abbiamo l'AgID - responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, nonché di esercitare le funzioni di accreditamento della conformità dei sistemi di intelligenza artificiale -; dall'altro, l'ACN - responsabile della vigilanza, dell'attività ispettiva e sanzionatoria dei sistemi di intelligenza artificiale -; assieme le due agenzie assicurano l'istituzione e la gestione degli spazi di sperimentazione normativa relativi alla IA (le cosiddette "regulatory sandboxes" introdotte dall'AI Act). Questa ripartizione, chiara sulla carta, potrebbe diventare molto più complessa in fase attuativa, rivelando alcune potenziali sovrapposizioni dal carattere incerto: ad esempio, le attività di definizione delle procedure per l'accreditamento dei produttori dei sistemi di IA (AGID) e quelle repressive di ispezione e sanzione nei confronti di tali sistemi (ACN). Un altro potenziale effetto negativo della duplicazione di autorità è la maggior difficoltà nella rappresentanza unitaria dell'Italia nelle sedi concertative europee, dove viene decisa gran parte della politica attuativa e regolatoria ed in cui siederanno due diversi organismi distinti per tema trattato -.

Come dicevo il tema ha suscitato un certo dibattito: da un lato, vi è stato chi ha proposto l'ipotesi di costituire un soggetto ad hoc per gestire il tema IA; soluzione che francamente appare ancora più complessa, dispendiosa e creatrice di potenziali

sovrapposizioni con le competenze delle altre autorità già esistenti; dall'altro lato, nel parere recentemente espresso dall'Autorità Garante della Protezione dei dati personali sul disegno di legge del governo [Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale - 2 agosto 2024 [10043532], il Garante ha ribadito come opportuno "*integrare l'articolo prevedendo, in fine, che AgID e ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati, richiedendo altresì il parere dell'Autorità rispetto a fattispecie, al loro esame, che coinvolgano aspetti di protezione dei dati*.". La proposta di emendamento in effetti muove da una constatazione realistica: il "carburante" fondamentale che alimenta l'industria dell'IA sono i dati - e non solo quelli personali -; dunque, un'adeguata considerazione di questi profili non potrà essere evitata e di qui nasce la richiesta di coinvolgere a pieno titolo anche il GPDP, che però nel disegno di legge non sembra avere responsabilità dirette. Infine, in conclusione, vi è anche da considerare le attuali attribuzioni di altre due autorità indipendenti che si sono attivamente occupate del tema dell'IA: l'Autorità per la concorrenza e il mercato (AGCM) e l'Autorità per la Garanzia delle comunicazioni (AGCOM); entrambe sono coinvolte come autorità di regolazione in numerosi settori - il mercato in genere e le telecomumicazioni in particolare - in cui il ruolo dell'IA è assolutamente rilevante.

Questa constatazione, infine, conduce alla seconda riflessione che suscita la scelta di individuare in AGID e ACN, le autorità nazionali in materia di IA: il fatto che entrambe siano "agenzie" governative e non "autorità indipendenti", ovverosia espressioni dirette del potere esecutivo, rispetto a soggetti che garantiscano maggior regime di indipendenza; va ricordato, infatti, che il Regolamento dell'AI act richiede che le *autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento"*.

***

ALESSANDRO STERPA - La "legge europea" e l'IA "per scopi esclusivamente militari"

A seguito dell'introduzione della regolazione europea sull'IA uno dei profili di maggiore discussione riguarda l'eccesso – per alcuni – piuttosto che la carenza – per altri – di regole per un settore che è caratterizzato da una potenzialità divergente: migliorare o compromettere le libertà degli individui. C'è chi accusa l'Unione europea di aver ecceduto con un impianto regolatorio che lascerebbe altrove, quindi non nel nostro continente, il rapido sviluppo e quindi la concreta disponibilità dell'IA; disponibilità e quindi conoscibilità dell'IA che costituiscono elementi prodromici sia ad ogni contro-rimedio tecnologico che ad ogni regolazione adeguata.

In pochi, in ogni caso, ricordano che la "legge europea" prevede un'isola "solamente lambita" (direbbe Arturo Carlo Jemolo) dalle prescrizioni europee e – forse – nazionali: l'art. 2 del Regolamento (UE) 2024/1689 prevede espressamente l'atto "*non si applica ai sistemi di IA sviluppati o usati per scopi esclusivamente militari*".

Non può non venire in mente che gli sviluppi più importanti della rivoluzione digitale sono avvenuti proprio in ambito militare, prima con la rete internet e poi con la sua apertura ed implementazione; che il settore militare abbia costituito l'ambiente ottimale di sviluppo di strumenti tecnologici che scomponessero e ri-componessero la complessità umana ce lo ricorda anche Alan Turing che lavorò per le forze armate britanniche al fine di decodificare Enigma, la innovativa macchina analogica con la quale i nazisti cifravano i messaggi militari. Proviamo a porre domande sul tema segnalato.

Prima di tutto la congiunzione "o" presente nel testo ci fa dire che la mancata applicazione del regolamento non riguarda i sistemi di IA "sviluppati *e* usati" ma una gamma più ampia: la "legge europea" non si applica ai sistemi di IA sviluppati in sede militare ma non necessariamente in essa impiegati e a quelli non sviluppati in sede militare e ma in quella sede comunque impiegati.

Ciò significa, a quanto pare, che le aziende interessate potranno avvalersi di deroghe al regolamento sull'IA qualora lo sviluppo sia ad "esclusivo" scopo militare, ma – ci chiediamo – anche che le tecnologie militari possano essere impiegate in sede non (strettamente) militare pur sviluppate fuori dai canoni del regolamento? Si apre, in poche parole, una questione di fondo: come regolare la circolazione dei sistemi di IA tra mondo militare e non militare, potenzialmente nel doppio senso di marcia. Occorre capire l'avverbio "esclusivamente" – dunque – quale effetto può concretamente avere sulla dinamica delle tecnologie duali che già hanno ampiamente caratterizzato la dialettica tra mondo militare e non militare.

Un secondo aspetto di riflessione riguarda la tipologia di sviluppo tecnologico a cui facciamo riferimento. È noto, infatti, che il rapporto tra esigenze militari e imprese è sempre stato del tutto peculiare, anche per deroghe ammesse, nell'ambito di altri apparati di regole dalla concorrenza alla trasparenza. Il punto di novità in questo caso parrebbe essere quello della dimensione immateriale dello sviluppo e della produzione industriale dell'IA. Come è facile immaginare, un conto è costruire un'arma o un componente d'arma con una evidente dimensione materiale e con materie prime tracciabili e definirne le regole con riguardo a standard di produzione, segretezza industriale e di sicurezza nazionale. Cosa diversa è il settore informatico che, salvo le impattanti infrastrutture per "farlo girare" e il grande consumo di energia a regime, può in piccolo e diffusamente sia sviluppare l'IA che produrre gli *output* più differenti. Si pensi alla complessità che genera già in tal senso la protezione del "perimetro" di sicurezza *cyber*.

Terzo aspetto, che ai primi due si connette, riguarda l'ampiezza della deroga per "scopi militari" visto che non si esaurisce in essi la "sicurezza nazionale"; peraltro nei singoli Paesi membri l'assetto dei sistemi di *intelligence* non è identico: in alcuni è

appannaggio delle strutture civili e in altri di quelle militari, salvo le inevitabili connessioni e collaborazioni.

La regolazione nell'ambito militare dell'IA è, ci sia permesso sottolinearlo, non solamente un tema "militare" ma anche un tema – più generale – di sicurezza nazionale.

Il regolamento sull'IA cita la sicurezza nazionale solamente in materia di riservatezza, prevedendo che "*nel momento in cui i sistemi di IA ad alto rischio* […] *sono utilizzati dalle autorità di contrasto o dalle autorità competenti in materia di immigrazione o di asilo, le informazioni scambiate in via riservata tra le autorità nazionali competenti e tra le autorità nazionali competenti e la Commissione non sono divulgate senza previa consultazione dell'autorità nazionale competente e dell'utente che hanno prodotto tali informazioni, qualora tale divulgazione rischi di compromettere gli interessi pubblici e di sicurezza nazionale*".

La questione appare essere di più ampio impatto però visto che il TUE prevede che la materia della sicurezza nazionale sia di esclusiva spettanza dello Stato: l'UE "*rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*" (art. 4, comma 2).

Si tratta di una competenza, quella riservata allo Stato in materia di sicurezza nazionale, che è completata da altre previsioni europee (art. 346 del TFUE) con la conseguenza, ad esempio, del condizionamento delle regole in materia di *procurement* pubblico in deroga parziale al principio di concorrenza nel mercato europeo.

La non applicabilità del regolamento sull'IA agli scopi militari, quindi, non può non essere associata a quella che si ricava dalla sicurezza nazionale quale materia di competenza degli Stati.

La Corte costituzionale ci ha ben spiegato che la sicurezza nazionale consiste nella difesa dell'assetto costituzionale repubblicano e dei suoi valori fino alla esistenza stessa dello Stato. Si tratta di un compito che non è di sola competenza delle forze armate ma, come sappiamo, anche dell'apparato di *intelligence* che fornisce – anche grazie alle qualificate competenze del settore militare – informazioni decisive per le decisioni politiche. Verrebbe da dire che quella deroga a favore degli "scopi esclusivamente militari" non possa non includere (o dare per scontata) anche la difesa "non militare" della sicurezza nazionale.

Come si concilia questa "riserva statale" per la sicurezza nazionale e per il settore militare in ambito di IA – tecnologia che ha un forte impatto sulla difesa e sulla sicurezza nazionale – con la costruzione di una politica estera e di sicurezza comune di cui all'art. 42 TUE? Rischiamo che in un settore dove contano investimenti e sicurezza si proceda in Europa su base nazionale senza dare corso a economie di scala e a processi di sviluppo e impieghi comuni? Oppure resta aperta la strada della collaborazione grazie agli Stati che, a geometrie variabili, vorranno attuarla, come già riconosce l'art. 42 TU in ambito di sicurezza comune quando si riferisce alla Nato e in quella, non formalizzata, dei servizi di *intelligence*?

Potrà, infine, questa "riserva ampia" in deroga alla "legge europea" permettere di recuperare una dimensione europea di azione sullo sviluppo dell'IA e, quindi, costituire un nucleo per rilanciare la comune difesa europea?

***

I PARTECIPANTI AL FORUM

Francesca Bailo, Professoressa associata di Diritto costituzionale e pubblico – Università di Genova

Giovanna De Minico, Professoressa ordinaria di Diritto costituzionale e pubblico – Università degli Studi di Napoli Federico II

Costanza Nardocci, Professoressa associata di Diritto costituzionale e pubblico – Università degli Studi di Milano

Edoardo Raffiotta, Professore associato di Diritto costituzionale e pubblico – Università degli Studi di Milano Bicocca

Andrea Simoncini, Professore ordinario di Diritto costituzionale e pubblico – Università degli Studi di Firenze

Alessandro Sterpa, Professore associato di Diritto costituzionale e pubblico – Università degli Studi della Tuscia