NOTE INTORNO AL (FUTURO) ARTIFICIAL INTELLIGENCE ACT. PROSPETTIVE COSTITUZIONALI E SFIDE DELL'IMMIGRAZIONE NELL'ECOSISTEMA DIGITALE*

di Michela Tuozzo**

Abbiamo perciò il dovere di allargare lo sguardo e di orientare la ricerca tecnico-scientifica al perseguimento della pace e del bene comune, al servizio dello sviluppo integrale dell'uomo e della comunità. La dignità intrinseca di ogni persona e la fraternità che ci lega come membri dell'unica famiglia umana devono stare alla base dello sviluppo di nuove tecnologie e servire come criteri indiscutibili per valutarle prima del loro impiego, in modo che il progresso digitale possa avvenire nel rispetto della giustizia e contribuire alla causa della pace. Gli sviluppi tecnologici che non portano a un miglioramento della qualità di vita di tutta l'umanità, ma al contrario aggravano le disuguaglianze e i conflitti, non potranno mai essere considerati vero progresso.

L'intelligenza artificiale diventerà sempre più importante. Le sfide che pone sono tecniche, ma anche antropologiche, educative, sociali e politiche.

Papa Francesco, *Intelligenza artificiale e pace*

La tecnologia ha sempre cambiato gli assetti economici e sociali.

Adesso, con l'intelligenza artificiale che si autoalimenta, sta generando un progresso inarrestabile.

Destinato a modificare profondamente le nostre abitudini professionali, sociali, relazionali.

Ci troviamo nel mezzo di quello che verrà ricordato come il grande balzo storico dell'inizio del terzo millennio. Dobbiamo fare in modo che la rivoluzione che stiamo vivendo resti umana. Cioè, iscritta dentro quella tradizione di civiltà che vede, nella persona - e nella sua dignità - il pilastro irrinunziabile.

Sergio Mattarella, *Messaggio di fine anno del Presidente della Repubblica*

To put it more metaphorically, the world provides the data, but we generate the information from the data, and the information is not a copy or a mirror image of the source of the data.

We have no direct epistemic access to the *noumenon*, we know only the phenomena.

Luciano Floridi, *On two philosophical earworms (series: notes to myself)*

1. Introduzione. Il 2023 si è contraddistinto, tra le altre cose, per essere stato l'anno nel quale si è registrato il record globale della regolazione sull'intelligenza artificiale (da ora in

* *Sottoposto a referaggio*. L'articolo si inserisce nelle attività di ricerca svolte nell'ambito del Progetto PNRR MUR: FAIR – Future AI Research – PE000013.

** Ricercatrice t.d., lett. *a)*, di Diritto costituzionale – Università di Napoli Federico II.

avanti IA)[1].
Il processo legislativo più avanzato è quello dell'Unione Europea con la *Proposta di regolamento sull'armonizzazione delle regole sull'Intelligenza artificiale*[2], che, nel momento in cui si licenzia il lavoro, è stato approvato dal Parlamento europeo e dal Consiglio dell'Unione europea, dopo l'accordo raggiunto il 9 dicembre 2023 durante i triloghi[3].
Tuttavia, il fenomeno non si limita all'Unione. Anche quei Paesi che tradizionalmente mostravano resistenza a regolare Internet stanno ora avviando discussioni in merito[4]. Ad esempio, il Presidente degli Stati Uniti ha emesso l'*Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* e *The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* a ottobre 2023[5]. Inoltre, il primo summit internazionale sulla sicurezza dell'intelligenza artificiale, tenutosi il 1° novembre 2023 a Bletchley, ha visto la firma della *Dichiarazione* omonima da parte dei leader di sistemi giuridici e politici, come gli Stati Uniti e la Cina, tra loro agli antipodi. Nel giugno del 2023, il Regno Unito ha adottato il documento politico *A pro-innovation approach to AI regulation*[6]. Anche la Cina ambisce ad a introdurre un suo AI Act[7]. Infine, il Consiglio d'Europa ha adottato nel maggio 2024 la prima Convenzione internazionale sull'intelligenza artificiale.
La tecnologia riflette norme, valori e rapporti di potere esistenti nella società, il che implica non solo che le tradizioni giuridiche di ogni ordinamento ne orienteranno l'attività regolatoria, ma che lo sviluppo tecnologico seguirà verosimilmente le asimmetrie esistenti tra *Global North* e *Global South*[8]. In altri termini, l'intelligenza artificiale produce, e produrrà, costi e benefici non uguali per tutti.
Questo studio intende esaminare in che modo il futuro Regolamento (da ora in avanti AI Act) affronti tali sfide, con uno sguardo specifico ai settori dell'immigrazione, dell'asilo e del controllo delle frontiere. Per dare un esempio del mutevole utilizzo dell'IA in questo settore si prenda il caso della previsione di una crisi migratoria. L'IA – alimentata da *big data*, dai dati

[1] Si vedano i risultati del rapporto HAI, *Artificial Intelligence Index Report 2023*, Chapter 6, 267 ss., che mette in luce l'incremento di atti legislativi che fanno riferimento all'IA dal 2016 al 2022, passando da 1 a 37 atti.
[2] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, 21.4.2021.
[3] Consiglio dell'UE, *Regolamento sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole per l'IA al mondo*, 9 dicembre 2023, all'url: https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/; European Parliament, *Artificial Intelligence Act: MEPs adopt landmark law*, 13.3.2024; Consiglio dell'Unione europea, *Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI*, 21.5.2024.
[4] La dottrina ha messo in luce il cd. *Brussels effect* in tale campo, J. Schuett, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023, 2.
[5] President Biden, *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, 30 ottobre 2023, all'url: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.
[6] UK Government, *A pro-innovation approach to AI regulation*, 2023, all'url: https://www.trade.gov/market-intelligence/uk-ai-regulations-2023.
[7] Per una panoramica sulle «geografie» dell'IA v. T. Ryan-Mosley, M. Heikkilä, Z. Yang, *What's next for AI regulation in 2024? The coming year is going to see the first sweeping AI laws enter into force, with global efforts to hold tech companies accountable*, in *MIT Technology Review*, 2024.
[8] «This also perpetuates the Global North as the locus of power and technological development, to be deployed in the Global South», così P. Molnar, *Technology on the margins: AI and global migration management from a human rights perspective*, in *Cambridge International Law Journal*, 2, 2019, 326.

derivanti da geolocalizzazione, dai *social network* e dai database su larga scala[9] – indica al decisore politico di prepararsi a tale evento. Questi potrebbe farlo in due direzioni opposte: evitare la saturazione del sistema di accoglienza e della macchina amministrativa, aprire canali di ingresso protetti, allocare in modo efficiente le risorse per la gestione dell'accoglienza, o viceversa nell'ottica di prevenire gli ingressi di migranti e richiedenti asilo, ampliando le ipotesi legislative delle politiche di *non-entrée*[10]. Le potenzialità del ricorso agli strumenti tecnologici presentano l'indubbio vantaggio di rafforzare il potere degli Stati sia in ordine all'esercizio della prerogativa dello *jus excludendi alios*, sia nella velocizzazione delle procedure per il riconoscimento dei diritti.

Lo sviluppo di sistemi algoritmici in questo settore si colloca nel più ampio fenomeno della digitalizzazione delle frontiere europee, che ha accelerato il suo sviluppo in risposta alla crisi dello spazio di libertà, sicurezza e giustizia del 2015. Crisi, quest'ultima, che ha scoperchiato il vaso di Pandora sulle fragilità dello spazio Schengen sotto il profilo della gestione dell'immigrazione e l'asilo, connotato da inefficienze amministrative degli Stati membri frontalieri e dall'insostenibilità degli oneri gravanti sugli stessi Stati[11].

È importante notare che mentre la digitalizzazione delle frontiere costituisce il presupposto per l'applicazione dei sistemi di IA, non vi è piena identificazione tra le due tecnologie, nel senso che attualmente l'implementazione dell'IA in ambito migratorio è meno estesa della digitalizzazione[12].

Alla luce di queste brevi premesse, due sono le traiettorie che si intende indagare in questo saggio: osservare il paradigma dell'*algorithm constitutional by design*[13] all'interno dell'AI Act e specificatamente le sue ricadute nel contesto migratorio. In tal senso, i due temi si intrecciano negli articoli 5 e 6 del futuro regolamento europeo e nella sua base giuridica orientata al funzionamento del mercato interno[14].

Il saggio si articola attorno all'analisi delle categorie di diritto costituzionale coinvolte, delineando così la prospettiva giuridica dalla quale si vuol esaminare la complessa relazione tra l'intelligenza artificiale e le dinamiche migratorie (§ 2). Nel solco di questo approfondimento, si procederà con una disamina degli elementi chiave dell'*AI Act* (§ 3), ponendo particolare attenzione all'ambito dell'immigrazione, delle frontiere e dell'asilo (§ 3.1). Infine, il testo si concentra su un caso specifico di studio riguardante il rilevamento delle emozioni alle frontiere, esaminando i profili critici connessi a tale pratica e a come si collochi in relazione al tema degli emergenti *neurorights* (§ 4).

2. Il costituzionalismo nell'ecosistema digitale. In riferimento al fenomeno dell'immigrazione e dell'asilo, la sfida che maggiormente si è imposta al costituzionalismo

[9] Sulla «datafication of migration management» D. Broeders, H. Dijstelbloem, *The Datafication of Mobility and Migration Management: the Mediating State and its Consequences*, in I. Van der Ploegand J. Pridmore (a cura di), *Digitizing Identities: Doing Identity in a Networked World*, London, 2016, 242.

[10] A. Beduschi, *International migration management in the age of artificial intelligence*, in *Migration Studies*, 3, 2021, 581. Per una panormica sugli attuali impieghi dell'intelligenza artificiale nelle politiche di immigrazione e asilo si veda D. Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, Oxford: Refugee Studies Centre, University of Oxford, 2023.

[11] D. Vitiello, *Le frontiere esterne dell'Unione europea*, Bari, 2020, 77 ss.

[12] A. Beduschi, M. McAuliffe, *Artificial Intelligence, migration and mobility: implications for policy and practice*, in *World Migration Report*, 2022.

[13] G. De Minico, *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal Giornale di BioDiritto*, 3 marzo 2021, *passim*.

[14] L'art. 3, par. 3, TUE è una disposizione complessa, perché l'Unione instaura il mercato interno ispirandosi a valori tra loro antagonisti: solidarietà e competitività. Sul tema A. Lucarelli, *Principi costituzionali europei tra solidarietà e concorrenza*, in *Liber amicorum per Pasquale Costanzo, Consulta online*, 2020.

moderno è stata quella del radicamento dei diritti nella dignità della persona, anziché nel suo rapporto con lo *status civitatis*. In tal modo, l'obiettivo è stato quello di recuperare l'originaria ispirazione universalistica nell'affermazione dei diritti umani per vagliare la legittimità delle scelte del legislatore, pur lasciandogli un margine nel differenziare la posizione giuridica del cittadino da quella dello straniero nel godimento dei diritti fondamentali[15].

I due valori, libertà ed eguaglianza, alla luce della quarta rivoluzione scientifica, incontrano nuove sfide per la realizzazione dell'aspirazione costituzionale di costruire una società in cui gli individui siano più liberi ed eguali che in qualsiasi altra forma di convivenza[16].

Per cogliere le trasformazioni in atto e la pervasività della rivoluzione del mondo dei *bit*, sia consentito uscire per un momento dalle categorie giuridiche, richiamando il pensiero di uno dei maggiori filosofi che abbiano speculato sulla tecnologia. Quest'ultimo ricorda come la più grande scoperta scientifica destinata a cambiare la comprensione del mondo e di noi stessi sia proprio quella dell'intelligenza artificiale. L'IA mette in discussione quella caratteristica che ha reso unica l'esperienza umana nell'universo: l'intelligenza del pensiero. Si apre la strada a una nuova consapevolezza: «Non siamo agenti newtoniani, isolati e unici, come una sorta di Robinson Crusoe su un'isola. Piuttosto, siamo organismi informazionali (*inforg*), reciprocamente connessi e parte di un ambiente informazionale (l'infosfera), che condividiamo con altri agenti informazionali, naturali o artificiali, che processano informazioni in modo logico e autonomo»[17].

Sul piano delle conseguenze politiche si assiste all'allontanamento dall'ordine disegnato dalla pace di Vestfalia – dove lo spazio fisico e giuridico coincidono e sono sottoposti al governo del potere statale – a favore di quello di Bretton Woods[18], dove attori non governativi sono riconosciuti come forze di influenza politica ed economica. Le ricadute specifiche nel nuovo ordine informazionale sono rappresentate dall'emersione di un nuovo soggetto, le *Information and Communication Technology* (da ora in avanti ICT), che mina il ruolo esclusivo dello Stato di collettore, produttore e controllore degli «strumenti tecnologici coinvolti nel ciclo di vita dell'informazione, i quali includono l'istruzione, il censo, le tasse, i dati raccolti dalla polizia, le leggi scritte, la stampa, i servizi segreti»[19]. Più criticamente i sociologi parlano di un nuovo capitalismo, che ha trovato il suo *habitat* nelle politiche neoliberiste e che si alimenta dei nostri comportamenti trasformati in dati. Si tratta del cd. «capitalismo della sorveglianza», che opera sfruttando l'asimmetria della conoscenza e del potere tra gli utenti e le *big tech*: «I capitalisti della sorveglianza […] Accumulano un'infinità di nuove conoscenze *da noi*, ma non *per noi*»[20].

---

[15] U. Allegretti, *Costituzione e diritti cosmopolitici,* in G. Gozzi (a cura di), *Democrazia, Diritti, Costituzione*, Bologna, 1997, spec. 144; M. Cuniberti, *La cittadinanza. Libertà dell'uomo e libertà del cittadino nella costituzione italiana*, Padova, 1997, 168 ss.; C. Corsi, *Lo stato e lo straniero*, Padova, 2001, 108 ss.; Id., *Immigrazione e crisi pandemica: quali implicazioni*, in *PasSaggi costituzionali*, 2, 2022, 266; G. Bucci, *Eguaglianza, immigrazione e libertà di circolazione nell'era della mondializzazione dell'economia*, in AA.VV., *Scritti in onore di Gianni Ferrara*, I, Torino, 2005, 393 ss.; G. Bascherini, *Immigrazione e diritti fondamentali. L'esperienza italiana tra storia costituzionale e prospettive europee*, Napoli, 2007, 108 ss.; V. Onida, *Lo statuto costituzionale del non cittadino,* in *Atti del XXIV Convegno annuale Cagliari, 16-17 ottobre 2009*, Napoli, 2010, *passim*; A. Ruggeri, *I diritti dei non cittadini. Tra modello costituzionale e politiche nazionali*, in C. Panzera, A. Rauti, C. Salazar, A. Spadaro (a cura di), *Metamorfosi della cittadinanza e diritti degli stranieri. Atti del Convegno internazionale degli studi di Reggio Calabria, 26-27 marzo 2015*, Napoli, 2016, 31 ss.; P. Bonetti, *Migrazioni e stranieri di fronte alla Costituzione: una introduzione*, in *Riv. Dir. Cost., Migrazioni*, 3, 2020, 19 ss.; E. Rossi, F. Biondi Dal Monte, *Diritto e immigrazioni. Percorsi di diritto costituzionale*, Bologna, 2022, 19.

[16] N. Bobbio, *Libertà ed eguaglianza*, Torino, 1995, *passim*.

[17] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. it., Raffello Cortina Editore, Milano, 2017, 106.

[18] *Ibidem*, cap. 8, *Politica. La nascita sei sistemi multi-agente*, spec. 197 ss.

[19] *Ibidem*, 198.

[20] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, trad. it., Luiss University Press, 2019, 23.

Eppure, le ICTs svolgono un ruolo per noi essenziale: mettere in comunicazione gli utenti e i sistemi computazionali, con una capacità di immagazzinare dati senza precedenti. Il numero di dati che quotidianamente viene generato dall'umanità e dalle nuove tecnologie è tale che si è coniato un nuovo termine per descrivere lo «tsunami [di dati] che sta sommergendo il nostro ambiente»[21]: lo *zettabyte*. Senza le ICTs ne verremmo sommersi, a questa complessità se ne aggiungono almeno altre due: le ICTs di ultima generazione non si pongono più tra uomo e natura, né tra uomo e tecnologia, bensì possono interagire autonomamente con altre tecnologie. Ciò significa che l'uomo è fuori dal processo comunicativo di dati[22]. Allo stesso tempo, l'acquisizione di più dati rientra tra le tecniche di riduzione dei pregiudizi (*debiasing*) volte a costruire sistemi algoritmici più accurati[23].

Se sul piano filosofico tale stato di cose induce a parlare di un nuovo ordine alla ricerca di un diverso equilibrio[24], sul piano costituzionale la dottrina è più prudente nell'attribuire alla nuova categoria valenza tecnico-giuridica.

Nel dibattito sul costituzionalismo digitale infatti c'è chi ritiene che il rapporto tra potere pubblico e operatori privati assuma caratteri inediti, per cui i soggetti privati non sono più solamente attori economici, bensì poteri in senso stretto, come mostra l'attenzione regolativa dell'Unione europea al fenomeno[25].

Il rischio, tuttavia, è di confondere causa ed effetto, mentre appare forse più utile distinguere il fenomeno dall'epifenomeno, collocando i poteri digitali tra le manifestazioni collaterali originatesi dal potere pubblico[26]. Diversa, infatti, è la questione su come i poteri digitali abbiano potuto acquisire il ruolo di *gatekeepers* dello spazio digitale a partire dalla cd.

---

[21] L. Floridi, Op. cit., 13.

[22] *Ibidem*, 36.

[23] I. Bartoletti, R. Xenidis, *Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination*, Council of Europe, 2023, 33.

[24] L. Floridi, op cit., 202.

[25] Si vedano le posizioni di O. Pollicino, (vice) *Potere digitale*, in *Enc. Dir., I tematici*, vol. V, 2023, 410 ss., il quale individua tale trasformazione in due processi: l'attivismo della Corte di giustizia sul riconoscimento degli effetti orizzontali della Carta dei diritti fondamentali UE e l'adozione di regole procedurali tese a limitare i problemi di opacità algoritmica. V. anche Id., *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 596 ss. G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022, 64 ss., individua l'ascesa del costituzionalismo digitale nel ruolo assunto dall'Unione europea nella società algoritmica. In particolare, l'Unione con la regolazione dei servizi digitali, della protezione dei dati e nell'ambito della libertà di espressione, mira a superare talune caratteristiche dell'ambiente digitale, come la delega indiretta dei poteri delle autorità pubbliche alle piattaforme private. V. anche Id., *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 1, 2021, 41 ss.; infine si v. anche la sistematizzazione proposta da E. Celeste, *Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges*, in *HIIG Discussion Paper Series*, 2, 2018, che vede nel costituzionalismo digitale una traslazione di quello moderno orientato alle specificità dell'ambiente digitale. Con la definizione di costituzionalismo digitale si identifica: «*the process of production of norms aiming to ensure the protection of fundamental rights and the balancing of powers within that context. In particular, I argue that, in this specific historical moment, such a process aims to produce a series of normative counteractions to address the alterations of the constitutional ecosystem generated by the advent of digital technology*» (p. 16). Infine, discute di costituzionalizzazione dei nuovi soggetti della società globalizzata G. Teubner, *Constitutional fragments. Social constitutionalism and globalization*, Oxford University Press, 2012, 42 ss. Più di recente anche F. Pizzetti, *Un nuovo costituzionalismo per l'UE digitale*, in *Agenda Digitale*, 9 gennaio 2024.

[26] In aperta critica alla categoria del costituzionalismo digitale: M. Luciani, *Relazione conclusiva*, in *La rivista del Gruppo di Pisa*, 3, 2021, 7-8, che parla di un costituzionalismo senza aggettivi, condividendo altresì le ragioni di M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, 3, 2021, spec. 746, che ritiene fuorviante la traslazione semantica in luogo dell'applicazione fedele del costituzionalismo moderno. In particolare, egli nota che tale approccio rischia di cristallizzare il potere degli attori privati, ritenendo che questi possano assicurare una maggiore protezione dei diritti fondamentali rispetto agli attori statali, accantonando altresì la legittimazione democratica degli organi che limitano e garantiscono i diritti.

regolazione dell'opportunità[27], ossia il liberismo digitale della prima stagione di Internet[28].
Per meglio intendere invece i motivi che inducono a dubitare dell'emersione di una nuova categoria giuridica si osservino le due caratteristiche portanti del costituzionalismo, come individuate con limpidezza da uno studioso[29], ossia resistenza e partecipazione. Queste ultime esprimono da un lato la necessità di limitare il potere politico che opprime le libertà e dall'altro lato quella di condividerlo: «Il costituzionalismo difende spazi di autonomia, ma costruisce anche unità politiche. Colloca i primi dentro le seconde, e nello stesso tempo impedisce alle seconde di assorbire i primi. Un compito richiama l'altro, in modo circolare e sostanzialmente indissolubile»[30]. La perdita dell'indissolubilità che ne deriverebbe finirebbe per alterare la costituzione dei poteri (e quindi dei diritti), alimentando così il distacco tra ordine giuridico e sociale[31].

Invero sembra più utile individuare una valenza descrittiva nell'ecosistema digitale le cui specificità richiedono ulteriori meccanismi per realizzare l'aspirazione alla tutela della dignità e la limitazione dei poteri, rispetto a quelli esistenti nel mondo degli atomi[32]. In altri termini, l'espressione coglie l'alterazione del modo in cui la persona gode dei diritti fondamentali amplificandone le possibilità di esercizio e minacciando il loro stesso godimento (sia nella formula della libertà «da» che in quella della libertà «di»); l'autorità riesce a tutelare gli interessi pubblici, esercitando i suoi poteri con un tasso maggiore di rapidità e certezza, ma anche di diffusione delle decisioni *biased*[33].

---

[27] Così definita da M. Pietrangelo, *Spazio digitale e modelli di regolazione*, in *Consulta online*, 3, 2023, 938.

[28] Sulla criticabilità *self-regulation* di internet in ordine alla realizzazione del *common good* si veda G. De Minico, *Internet e le sue fonti*, in *Osservatorio sulle fonti*, 2, 2013, 7 ss.; O. Pollicino, *Potere digitale*, cit., 428 ss.

[29] M. Fioravanti, *Il costituzionalismo nella dimensione sovranazionale: il caso europeo*, in Id., *Costituzionalismo*, Bari, 2008, anche all'url: https://www.astrid-online.it/static/upload/protected/anti/anti_costituzionalismo-nella-dimensione-sovranazionale_06_08.pdf, 2. Si veda N. Matteucci, *Costituzionalismo*, in *Enciclopedia delle scienze sociali Treccani*, 1992, all'url: https://www.treccani.it/enciclopedia/costituzionalismo_(Enciclopedia-delle-scienze-sociali)/.

[30] Id., *Costituzionalismo. Percorsi della storia e tendenze attuali*, Ed. Laterza, Bari-Roma, 2009, rist. 2012, Prefazione.

[31] G. Azzariti, *Diritto o barbarie: Il costituzionalismo moderno al bivio*, Bari-Roma, 2021, spec. 96 ss.

[32] Non parlano dell'autonomia di una nuova categoria costituzionale: G. De Minico, *Towards an "Algorithm Constitutional by Design"*, cit., spec. 398 ss., sostiene la necessità – per l'IA impiegata dai pubblici poteri – di garantire l'*algorithm Constitutional by design*, ossia un algoritmo che assicuri il rispetto del principio di non discriminazione e che assicuri la conoscibilità del codice sorgente per evitare l'effetto *black box*. Solo così il principio di legalità troverà applicazione anche nella decisione algoritmica e può sostenere il principio di eguaglianza: «*to be fair and equal, the algorithms must be regulated, and the crucial rule is that equal situations deserve the same treatment and different situations must receive a differentiated discipline. 'Substantive equality requires more than simply equal treatment' as treating groups identically may itself produce inequalities*», 402; A. Simoncini, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, in *BioLaw Journal – Giornale di BioDiritto*, 16 giugno 2021, 63 ss. secondo il quale la nuova realtà fenomenica, in cui la tecnologia «non è più soltanto un 'mezzo' […], ma, sempre più spesso, è essa stessa a prendere decisioni rilevanti per la persona umana e la sua libertà» (p. 69), necessita l'intervento di un diritto costituzionale ibrido che parli alla tecnologia.

[33] La specificità delle discriminazioni algoritmiche rispetto a quelle umane è data dalla sovrapposizione di più fattori: «*Algorithmic determinism is particularly problematic in relation to discrimination as predictive systems use correlations arising from historical discrimination (e.g., the gender pay gap) as quasi 'causal' bases for decision-making, thereby creating feedback loops. At the same time, AI and algorithmic systems are often non-transparent, might not be explainable, and the attribution of responsibility for discrimination is unclear. Because the source of these biases is not ultimately technological, they cannot be resolved using technology alone*», così I. Bartoletti, R. Xenidis, op. cit., 29. Sullo stesso tema v. anche Commissione europea, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, 19.2.2020: «Le distorsioni e le discriminazioni rappresentano un rischio intrinseco di qualunque attività sociale od economica. Il processo decisionale umano non è immune da errori e distorsioni. Queste stesse distorsioni, se presenti nell'IA, potrebbero tuttavia avere effetti molto maggiori e colpire o discriminare numerose persone in assenza dei meccanismi di controllo sociale che disciplinano il comportamento umano. Ciò può accadere anche quando il sistema di IA 'apprende' nel corso del suo funzionamento. In tali casi, in cui i risultati non potevano essere evitati o anticipati in fase di progettazione, i rischi deriveranno non da difetti nella progettazione originale

Da questa prospettiva non ci si interrogherà dunque sulla moltiplicazione dei centri di potere e sull'efficacia orizzontale dei diritti, bensì su come mantenere l'equilibrio costituzionale nel rapporto tra migrante/richiedente asilo e pubblica autorità, quando i sistemi di IA diventano *media* che interferiscono nell'esercizio dei diritti fondamentali. La circostanza indicata evidentemente arricchisce e complica il modo in cui i principi di legalità, del giusto procedimento e processo, della tensione verso la pari dignità sociale e l'eguaglianza sostanziale, del buon andamento e imparzialità della pubblica amministrazione, dell'indipendenza e autonomia dei giudici, vivono in un contesto socio-ambientale nel quale la digitalizzazione e l'automatizzazione sono parti integranti degli strumenti dell'ordine sociale.

A tal proposito, da un lato, si accolgono gli esiti cui è giunta la dottrina in merito ai principi che dovrebbero supportare gli sviluppi della digitalizzazione: *data justice*, *algorithmic transparency* e *human oversight*[34]; dall'altro lato, si impiega cautela, perché il rapporto autorità e libertà che percorra le nuove traiettorie tracciate solamente con la regolazione «della» tecnologia rischia di trascurare le «inedite dimensioni di conflittualità che si aprono attualmente su questi terreni»[35].

Nel momento in cui si licenzia il lavoro, tale analisi è supportata dall'attenzione legislativa maturata in sede europea e nazionale sugli aspetti indicati[36].

In particolare, questo contributo vuole concentrarsi sulla prospettiva originale del *legal framework* eurounitario[37]. Quest'ultimo recepisce giuridicamente il consenso etico sui valori

---

del sistema, bensì dagli effetti pratici delle correlazioni o dei modelli che il sistema individua all'interno di un ampio set di dati».

[34] E. Longo, A. Pin, *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale,* in *Diritto pubblico comparato ed europeo*, 1, 2023, 113-115.

[35] R. Nania, *Temi generali nello studio dei diritti fondamentali*, in Id. (a cura di), *L'evoluzione costituzionale delle libertà e dei diritti fondamentali*, Torino, 2013, 12.

[36] Con l'art. 30, d.lgs. n. 36/2023 (*Codice dei contratti pubblici*). La disposizione prevede che nell'ambito delle procedure automatizzate nel ciclo di vita dei contratti pubblici qualora le stazioni appaltanti e gli enti concedenti ricorrano all'IA adottino misure volte a garantire la trasparenza della procedura mediante l'accesso del codice sorgente (c. 2, lett. *a)*) e a prestazioni di assistenza e manutenzione per correggere errori ed effetti indesiderati derivanti dall'automazione (lett. b). Al comma 3 sono previsti ulteriori principi da osservare per l'adozione delle decisioni: conoscibilità e comprensibilità sulla logica utilizzata (lett. a); non esclusività della decisione algoritmica (lett. b); non discriminazione algoritmica (lett. c). Ulteriori oneri sono previsti, al comma 4, in capo alla stazione appaltante in merito alle misure tecniche per evitare fattori che comportano inesattezze dei dati e la minimizzazione del rischio di errori, compresi gli effetti discriminatori. La disposizione recepisce e amplia la portata dell'art. 22, reg. UE 679/2016 e la giurisprudenza del Consiglio di Stato sulle decisioni algoritmiche (su cui v. L. Carbone, *L'algoritmo e il suo giudice,* in J.-B. Auby, G. De Minico, G. Orsoni (a cura di), *L'amministrazione digitale. Quotidiana efficienza e intelligenza delle scelte*. Atti del Convegno 9-10 maggio 2022, Napoli, Federico II, Napoli, 2023, 111 ss.). Si tratta di una disposizione che guarda al futuro sviluppo dell'IA nel procedimento amministrativo, che al momento utilizza algoritmi di non apprendimento, come specificato da Consiglio di Stato, *Schema definitivo di Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante "Delega al Governo in materia di contratti pubblici"*, *Relazione agli articoli e agli allegati*, 7 dicembre 2022, 49. I principi in essa presenti «mirano a delineare la cornice giuridica di un fenomeno, insieme tecnologico, economico e sociale, di cui è imminente lo sviluppo e del quale saranno rilevantissime, e per molti aspetti imprevedibili, le implicazioni, anche di carattere giuridico», così G. Carlotti, *I principi nel Codice dei contratti pubblici: la digitalizzazione*, in *Giustizia-amministrativa.it*, 2023, 8-9. In tema anche D.U. Galetta, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in *Federalismi.it*, 12, 2023, ix.

[37] Come dimostrano: i due regolamenti sui servizi (*DSA*) e mercati digitali (*DMA*), rispettivamente reg. UE 2022/2065 e 2022/1925; la proposta di direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali COM(2021) 762 *final*; la proposte di direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale) COM(2022) 496 *final* e quella sulla responsabilità per danno da prodotti difettosi COM(2022) 495 *final*. Per una lettura complessiva del *DSA*, *DMA* e *AI Act* v. L. Torchia, *I poteri di vigilanza,*

del Libro bianco del 2020[38] e che si struttura intorno al punto di equilibrio tra tutela dei diritti e mercato dell'innovazione attraverso il *risk management approach*, «come modello giuridico *tout-court* nel quale i valori dell'Unione rappresentano il limite di tenuta del sistema al quale istituzioni e individui riferiscono la propria identità 'europea'»[39].
In tal senso può quindi affermarsi che le componenti del costituzionalismo si stiano adattando alla sfida del presente, incorporando nel suo *ethos* attuale, opportunamente aggiornato «l'istanza originaria di controllo del potere» e «anche ed ulteriormente il limite allo strapotere dell'economico»[40].

3. Il (futuro) regolamento europeo sull'intelligenza artificiale: opportunità e limiti. La proposta di regolamento sull'intelligenza artificiale segue un approccio proporzionato, basato sulla gestione dei rischi e costituito da un processo interattivo continuo eseguito nel corso dell'intero ciclo di vita di un sistema di IA. L'*AI Act* introduce a tal proposito non solo un sistema di gestione dei rischi nel corso di tale ciclo nella sua interezza (art. 9), ma anche un meccanismo della responsabilizzazione lungo la catena di valore tra fornitori, distributori, importatori, operatori o altri terzi (art. 25). Tale attenzione «dinamica» ai sistemi di IA è costruita per differenza rispetto al quadro giuridico sulla sicurezza dei prodotti che rimangono «stabili» nel tempo dopo la distribuzione nel mercato[41].
Il modello legislativo scelto si ispira sia all'approccio di mitigazione del rischio *by design* del regolamento sulla protezione dei dati personali, sia alle regole sulla sicurezza dei prodotti.
Il punto di partenza è dato dalla base legislativa dell'atto: l'art. 114 del TFUE. Disposizione che consente all'Unione di armonizzare applicazioni eterogenee riguardanti i requisiti tecnici dei sistemi di IA, che compromettono il buon funzionamento del mercato interno, viste la complessità tecnica, la varietà dei prodotti e dei servizi interconnessi, nonché la moltitudine di attori privati e pubblici (v. il caso CGUE, *United Kingdom of Great Britain and Northern Ireland v. European Parliament and Council of the European Union*, C-217/04, par. 63).
Allo stato attuale, la disarmonia normativa è stata una delle cause della frammentazione del mercato con plurimi effetti negativi, poiché l'assenza di standard di sicurezza comuni e di *clear red lines* si riflette a cascata i) sulle imprese più piccole, che non possono sopportare i costi derivanti dalla presenza in mercati differenti, ii) sull'Unione europea, che non riesce a trovare un proprio spazio di sovranità digitale, e, infine, iii) sugli attori statali e sui cittadini, che faticano a costruire un rapporto di fiducia con i sistemi di IA.
L'atto europeo cerca quindi di trovare un punto di equilibrio tra quattro esigenze: assicurare che l'IA immessa sul mercato sia sicura per la tenuta dei valori e dei diritti fondamentali; dotare il sistema di una chiara *governance* delle istituzioni europee e nazionali per garantire la *compliance*; favorire gli investimenti nell'innovazione tecnologica tramite la certezza del diritto; sviluppare il mercato unico europeo.
Come anticipato, tale complessa scelta è individuata in una normativa di carattere

controllo e sanzionatori nella regolazione europea della trasformazione digitale, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1101 ss.

[38] Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 *final*.

[39] M. Catanzariti, *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, in *Società Mutamento Politica*, 25, 2022, 74.

[40] S. Prisco, *Costituzionalismi antichi e moderni tra strutture invarianti e specificità storiche*, in *Diritti fondamentali*, 2, 2012, 27, che così si riferisce alle radici antiche del costituzionalismo moderno da consegnare alle sfide del futuro.

[41] Commission Staff Working Document Impact Assessment, *Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, {COM(2021) 206 final} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

precauzionale, che si applica in ragione del rischio e in modo orizzontale a tutti i rami del diritto.

Definito l'approccio, il futuro regolamento individua quali siano i sistemi di IA a cui esso si rivolge attraverso la definizione giuridica contenuta nell'art. 3. L'IA è, dunque, un «sistema basato su macchine, progettato per operare con vari livelli di autonomia e che può mostrare un'adattabilità dopo l'implementazione, e che, per obiettivi espliciti o impliciti, deduce, dall'input che riceve, come generare output quali contenuti, previsioni, contenuti, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali»[42]. Una definizione che si connota per la presa di consapevolezza che i risultati della macchina non necessariamente coincidono con gli *input* e gli obiettivi umani, oltre che per una valutazione dell'impatto ambientale che va oltre l'antropocentrismo[43].

Il cuore del regolamento è costituito dalla categorizzazione dei sistemi di IA e quindi dalla modulazione delle regole in esso previste, a seconda del grado di rischio. Per tale motivo, sono vietati i sistemi di IA particolarmente dannosi (art. 5), in quanto in contrasto con la protezione della salute, della sicurezza, dei diritti fondamentali (art. 1), mentre è stabilita una metodologia per identificare i sistemi di IA «ad alto rischio» (art. 6 e all. III), verso cui è diretto il fitto corpo di regole riguardanti i dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la sorveglianza umana nonché la robustezza e la precisione (artt. 10-15). Per quei sistemi che invece non rientrano nelle categorie precedenti si mira alla creazione di codici di condotta, per incoraggiare i fornitori ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio. Infine, sono previsti obblighi minimi di trasparenza (art. 50) per le IA non ad alto rischio, ma che sono destinate a interagire autonomamente con le persone; per i sistemi di identificazione biometrica e di riconoscimento delle emozioni non rientranti nei precedenti artt. 5 e 6; nonché per le IA che producono *deep fake* e quelle generative. Infine, nel corso dei lavori legislativi, proprio la diffusione dell'IA generativa ha portato ad una ulteriore categorizzazione con obblighi *ad hoc*, a metà strada tra quelli previsti agli artt. 10-15 e quelli individuati all'art. 50, per i sistemi di *General-purpose artificial intelligence technologies* (artt. 51 ss.).

Il quadro della categorizzazione del rischio diversifica non solo diritti e doveri, ma anche il relativo sistema di controlli *ex ante* (artt. 27 e 43) ed *ex post* (Capo IX), nonché quello dell'efficacia delle attività svolte dall'*AI Board* e dall'Autorità nazionale di vigilanza (art. 66 e 70) e della reclamabilità delle decisioni dell'autorità nazionale di controllo (artt. 85 e 86). Infatti, il regolamento è rivolto principalmente ai sistemi individuati dall'art. 6 e dall'All. III, per cui le IA con rischio basso sono perlopiù libere dai vincoli indicati, mentre per quelle ad alto rischio i fornitori devono ridurne l'impatto verso la soglia di accettabilità (che non significa azzeramento del rischio), adottando misure in grado di assolvere agli obblighi dell'*AI Act*[44].

---

[42] Si noti la differenza con la versione elaborata dalla Commissione, che allo stesso articolo definisce così l'IA: come un software che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono. L'attuale versione differisce parzialmente anche da quella elaborata dal Parlamento europeo a giungo 2023, che invece recitava: «un sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare output quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali». Il testo attuale ingloba anche i sistemi basati su macchine, come i robot, e pone l'accento sulle trasformazioni del sistema una volta uscito dalle mani del fornitore.

[43] Riflette sull'opportunità di una definizione orientata all'ambiente digitale L. Floridi, *On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence*, in *Philosophy & Technology*, 2023, 86 ss.

[44] J. Schuett, op. cit., 4.

L'impianto generale dell'atto[45] risulta *prima facie* in linea – almeno per le IA ad alto rischio – con i tre principi individuati nel precedente paragrafo, ossia con la previsione di disposizioni *ad hoc* sui dati e una loro *governance* (art. 10), la trasparenza e fornitura di informazioni agli utenti (art. 13) e la sorveglianza umana (art. 14). Allo stesso tempo si segnala un arretramento rispetto all'avanzamento sul piano dei valori e della difesa dei diritti, che il Parlamento aveva realizzato con gli emendamenti del giugno 2023 (a titolo di esempio si considerino la riformulazione di alcuni articoli chiave, come il 6 e il 27; l'eliminazione diritto a un ricorso giurisdizionale effettivo contro un'autorità nazionale di controllo e le modifiche della *governance*).

Rispetto a tale assetto emergono almeno due tipi di ostacoli su cui l'*AI Act* non interviene nello spirito dello *human in/on/out of the loop* e che, per motivi differenti, generano incertezze sull'affidabilità delle macchine costruite in adesione alle previsioni del futuro regolamento.

Il primo è quello relativo all'esistenza di un problema epistemologico – cioè della conoscenza tecnologica – che non può essere adeguatamente affrontato con le soluzioni giuridiche individuate. È il caso di quei sistemi di apprendimento automatico come quelli di *deep learning* con reti neurali che possono evolvere in seguito alla loro diffusione, con funzione e *output* che si basano su relazioni matematiche astratte, per i quali inoltre gli *input* specifici sono difficili da rintracciare per risalire alla catena di causalità. Ciò posto, tali sistemi risultano di difficile comprensione da parte dell'uomo; dunque, è impossibile svolgere l'attività di sorveglianza umana. Tali caratteristiche complesse e opache incidono sulla rendicontabilità e sulla spiegabilità del risultato algoritmico. In altri termini, le indicazioni sulla trasparenza e sulla supervisione umana, di cui rispettivamente negli artt. 13 e 14, perderebbero la loro efficacia garantistica, che non è recuperabile neppure tramite l'accesso al codice sorgente[46]. Il difetto di trasparenza si rifletterebbe infatti a sua volta sulla concretezza della supervisione umana e della spiegabilità dell'*output* (art. 86). Tale catena di incomprensibilità incide fatalmente sulla garanzia della sottoposizione alla legge del potere esecutivo e giudiziario, come è previsto agli artt. 97[47] e 111 Cost.[48]. È lecito dunque chiedersi come potrebbe l'autorità nazionale di vigilanza o quella giudiziaria risolvere *ex post* lo scarto tra

[45] Si vedano i commenti di M.E. *Kaminski, Regulating the Risks of AI*, in *U of Colorado Law Legal Studies Research Paper No. 22-21*, 1 ss.; C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2021, 415 ss. ; F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *dUE*, 3-4, 2021, 453 ss.; G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots In The Digital Age*, in *Common Market Law Review*, vol. 59, 2022, 473 ss.; S. Heiss, *Artificial Intelligence Meets European Union Law The EU Proposals of April 2021 and October 2020*, in *EuCML*, 6, 2021, 252 ss.; J. Schuett, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023, 1-19; A. Lucarelli, *Audizione XI Commissione Lavoro pubblico e privato*, 20 dicembre 2023, all'url: https://www.camera.it/application/xmanager/projects/leg19/attachments/upload_file_doc_acquisiti/pdfs/000/009/840/Lucarelli.pdf ; A. Alaimo, *Il Regolamento sull'Intelligenza Artificiale*, in *Federalismi.it*, 25, 2023, 133 ss.; S. Foà, *Intelligenza artificiale e cultura della trasparenza amministrativa. Dalle "scatole nere" alla "casa di vetro"?*, in *Diritto amministrativo*, 3, 2023, 515 ss.; C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in *Federalismi.it*, 2, 2024, 95 ss.

[46] La cd. apertura della *black box* di cui parla F. Pasquale, *The black box society. The secret Algorithms that control money and information*, Harvard, 2016, 40. Soluzione espressa nella giurisprudenza amministrativa italiana e altresì accolta nel riformato codice dei contratti all'art. 30 (v. nt. 36) e presente anche nella proposta di regolamento della Commissione all'art. 64. Tale disposizione è stata poi emendata dal Parlamento europeo e attualmente espunta dall'articolo.

[47] Significativo è il filone della giurisprudenza amministrativa italiana che si è sviluppato a partire dal Consiglio di Stato, n. 2270/2019: «la regola algoritmica deve essere non solo conoscibile in sé, ma anche soggetta alla piena cognizione, e al pieno sindacato, del giudice amministrativo» (par. 8.4).

[48] Sulla trasparenza e sulla motivazione come garanzie costituzionali C. Colapietro, *Gli algoritmi tra trasparenza e protezione dei dati personali*, in *Federalismi.it*, 5, 2023, 158.

comprensibilità della tecnica e quella umana.
L'art. 86, pur affermando il diritto alla spiegazione dei singoli processi decisionali, non indica quali saranno le conseguenze giuridiche della decisione *in*comprensibile. Ad ogni modo, la presenza di *outputs* oscuri genera due opposti esiti negativi: la disutilità di ricorrere all'IA da parte dei pubblici poteri, perché il supporto offerto dalla macchina, in quanto opaco e non sorvegliabile, sarebbe inutilizzabile; o, all'opposto, il rischio di una resa dell'autorità terza all'imperscrutabilità della macchina, creando così una zona tecnologica franca dal principio di legalità e dal contrappeso giudiziario. Tali esiti, a ben vedere, finirebbero per rovesciare i due paradigmi che il regolamento cerca di realizzare, vale a dire la certezza del diritto e la fiducia nell'IA.
L'opacità algoritmica non rientra tuttavia tra le ipotesi di sistemi di IA vietati, con la conseguenza che la decisione finale sarà a sua volta fisiologicamente oscura, con intuibili ricadute sulla tutela delle libertà che l'IA dovrebbe invece contribuire a realizzare.
Sul piano tecnico sono stati segnalati gli attuali limiti dell'*explainable AI,* ossia quelle tecniche di spiegabilità successiva che mirano a rendere comprensibile la relazione *input-output* dell'algoritmo. Esse in realtà restano approssimazioni imperfette che descrivono *ex post* il modello decisionale. Gli algoritmi migliorano la propria efficacia diventando più autonomi e complessi, ma proprio l'aumento di tali due caratteristiche compromette la completezza e l'accuratezza della spiegabilità della logica interna del sistema[49].
L'art. 13 non utilizza il termine spiegabilità bensì la «sufficiente trasparenza» che garantisca al *deployer* la interpetabilità dell'*output*. Diversamente l'art. 86, similmente all'art. 22, par. 3, reg. 679/2016[50], stabilisce che qualsiasi persona interessata ha diritto di ricevere dal *deployer* spiegazioni chiare e significative sul ruolo dell'IA nella procedura decisionale. Si tratta quindi di obblighi dal diverso contenuto e destinatario, la cui portata prescrittiva potrebbe non coincidere con le tecniche di *explainable AI* (del resto il regolamento non vi si riferisce espressamente).
In realtà dal regolamento emergono differenti significati di trasparenza[51], che rispecchiano tutto sommato l'assenza di una tassonomia comune delle tecniche informatiche. Secondo alcuni non vi è distinzione tra spiegabilità e interpretabilità, ma correlazione ossia un rapporto mezzo-risultato: le spiegazioni sono lo strumento che consentono l'interpretazione del risultato[52]. L'assenza di un linguaggio comune finisce così per avere conseguenze negative sul piano della certezza giuridica.
Il secondo limite del futuro regolamento riguarda invece la democraticità nella definizione di tutti i suoi articoli. In particolare, nell'AI Act la concreta individuazione di standard armonizzati, il cui rispetto garantisce l'accesso alla certificazione di conformità con i requisiti del suo titolo III, quindi l'immissione sul mercato interno, è posta fuori della procedura

[49] C. Panigutti *et al.*, *The role of explainable AI in the context of the AI Act*, in *FAccT '23*, June 12–15, 2023, 1143 e ivi per l'identificazione degli ostacoli. Sul trade-off tra performance algoritmica e spiegabilità T. Tzimas, *Algorithmic Transparency and Explainability under EU Law*, in *European Public Law*, 4, 2023, spec. 393.
[50] In chiave prospettica dovrà tenersi in considerazione quanto affermato nel caso *Ligue des droits humains* (causa C-817/19) dalla Corte di giustizia: «le autorità competenti devono assicurarsi che l'interessato, senza necessariamente consentirgli, nel corso del procedimento amministrativo, di avere conoscenza dei criteri di valutazione prestabiliti e dei programmi che applicano tali criteri, sia in grado di comprendere il funzionamento di tali criteri e di tali programmi, in modo da poter decidere, con piena cognizione di causa, se esercitare o meno il suo diritto a un ricorso giurisdizionale garantito dall'articolo 13, paragrafo 1, della direttiva PNR, al fine di contestare, se del caso, il carattere illecito e, in particolare, discriminatorio di detti criteri» (p. 210).
[51] Interessante la ricostruzione di quattro diversi significati di trasparenza nell'AI Act proposta da A. Kiseleva, *Making Ai's transparency transparent: notes on the EU Proposal for the AI Act*, in *European Law Blog*, 29.7.2021.
[52] In tema A. Kiseleva, D. Kotzinos, P. De Hert, *Transparency of AI in Healthcare as a Multilayered System of Accountabilities: Between Legal Requirements and Technical Limitations*, in *Front. Artif. Intell*, 5, 2022, 6.

legislativa in corso. L'art. 40 aderisce alla normativa europea sulla sicurezza dei prodotti del *New Legislative Framework* (NLF), per cui mentre il Regolamento ha stabilito quali obiettivi raggiungere, le *European Standards Organisations* «*define how to reach them*»[53].
La richiesta di normazione rivolta a tali organizzazioni riguarda aspetti essenziali, come la gestione del rischio nell'intero ciclo di vita dell'IA, i dati e la loro *governance*, le attività legate a robustezza, la trasparenza e la sorveglianza umana, fino alle competenze che deve possedere chi si occupa della valutazione della conformità[54].
A ciò si aggiunge che come per la NLF si ritiene più opportuno che l'attività di certificazione sia svolta dallo stesso manifattore del prodotto – nel nostro caso il *provider* – anziché procedere con il rilascio di una certificazione di un ente pubblico[55].
Attraverso siffatto sistema, il «vero ruolo nomotetico»[56] finisce per essere affidato agli standard armonizzati. Saranno questi ultimi a stabilire in concreto il livello di accettabilità del rischio delle macchine, spostando fuori del circuito democratico aspetti cruciali dell'intero impianto dell'AI Act.
Preoccupazioni simili, seppure in un diverso contesto, sono già emerse rispetto agli atti normativi dal contenuto tecnico-scientifico[57] (*science based* o *science related*) nell'emergenza pandemica. Per essi la regola di comportamento è stata individuata in un ambito extra-giuridico, limitando lo spazio di discrezionalità del bilanciamento del legislatore e il metabilanciamento della Corte costituzionale[58]. La dottrina aveva peraltro messo in luce la necessità che i Comitati tecnico-scientifici garantissero indipendenza e trasparenza dai portatori di interessi e dalla politica[59].
Mutatis mutandis, non si può che nutrire lo stesso timore a carico delle organizzazioni europee suddette, che difettano dei presupposti agli artt. 11 e 117, co. 1 Cost. e oltretutto svolgeranno

[53] M. Gornet, *The European approach to regulating AI through technical standards*, 2023, 3. Cfr. il testo anche per approfondire la natura di tali organizzazioni. In tema anche G. Mazzini, S. Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. Camardi (a cura di), *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche - Ca' Foscari Venezia, 25-26 novembre 2021*, Padova, 2023, disponibile anche su SSRN: https://ssrn.com/abstract=4098809 or http://dx.doi.org/10.2139/ssrn.4098809.
[54] *Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence*, 5/12/2022.
[55] M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 4, 2021, 102; in tema si veda la proposta di inserire un sistema di licenze prima dell'immissione dell'IA sul mercato di G. Malgieri, F. Pasquale, *Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology*, in *Computer Law & Security Review*, 2024, 11 ss.
[56] Così G. Resta, *Cosa c'è di "europeo" nel Regolamento AI?*, in *Il diritto dell'informazione e dell'informatica*, 2, 2022, 341; e M. Veale, F. Zuiderveen Borgesius, op. cit., 105, scrivono: «*In theory, providers do not have to follow such harmonised standards. Instead, providers could interpret the Draft AI Act's essential requirements for themselves. This is easier said than done. Harmonised standards are both cheaper for producers, and a safer bet. They are not as voluntary as the Commission argues. Essential requirements are often not realistically suitable for direct application. Harmonised standards often function as a necessary point of reference for compliance through essential requirements. In the Draft AI Act, the requirement to consult harmonised standards is explicit. Consequently, standardisation is arguably where the real rule-making in the Draft AI Act will occur*».
[57] Per un approfondimento A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018, spec. 10 ss.; S. Penasa, *Alla ricerca di un lessico comune: inte(g)razioni tra diritto e scienze della vita in prospettiva comparata*, in *DPCE online*, 3, 2020, 3307 ss.
[58] In tema cfr. R. Bin, *La Corte e la scienza*, in *http://www.robertobin.it/ARTICOLI/cortescienza.htm*, che parla di *self restraint* della Corte dinanzi a fatti e dati scientifici.
[59] A. Iannuzzi, *Leggi* "science driven" *e CoViD-19. Il rapporto fra politica e scienza nello stato di emergenza sanitaria*, in *BioLaw Journal*, special issue 1, 2020, 133 e Id., *Il diritto capovolto*, cit., 173 ss.; In generale sul rapporto tra scienza e diritto E. Castorina, *Scienza, tecnica e diritto costituzionale*, in *Rivista AIC*, 4, 2015, spec. 18-21,

un compito che non è né neutrale[60], né meramente esecutivo. All'opposto, l'identificazione privatistica degli standard armonizzati determinerà il concreto all'equilibrio tra innovazione, tutela dei diritti fondamentali e sfruttamento economico degli algoritmi.

3.1. (segue) La categorizzazione del rischio dell'IA per le politiche migratorie. Per ciò che concerne il *focus* tematico di questo scritto è utile in premessa identificare le IA attualmente in uso nel controllo e nella sicurezza delle frontiere. Si tratta di sistemi rivolti all'identificazione biometrica; al rilevamento delle emozioni; alla valutazione algoritmica del rischio; alla previsione dei movimenti di immigrazione[61]. Tali attività corrispondono alle diverse fasi in cui il migrante, il richiedente asilo o il rifugiato attraversa la frontiera; infatti le suddette IA svolgono compiti che vanno dai controlli d'identità prima della partenza, al supporto per la presentazione e l'elaborazione delle domande di visto, al miglioramento delle procedure di frontiera, all'analisi dei dati per il rilascio dei visti, nonché alla previsione delle tendenze migratorie.

Alla luce delle opportunità e dei rischi connessi all'utilizzo dell'intelligenza artificiale alle frontiere[62], si può osservare in quale modo il futuro regolamento sull'intelligenza artificiale salvaguardi le prime e mitighi i secondi.

A questo scopo occorre partire dalla categorizzazione delle azioni connesse ai fenomeni migratori, distinguendo quanto stabilito nella *Proposta* di aprile 2021, dai successivi mutamenti intervenuti con gli emendamenti approvati dal Parlamento europeo a giugno 2023 e il testo finale adottato dal Parlamento europeo e Consiglio UE, rispettivamente, il 13 marzo e 21 maggio 2024.

Sin da subito va evidenziato che la parte del regolamento relativa al sistema dei controlli *ex ante* ed *ex post* non è stata emendata in modo significativo. L'art. 43 disciplina lo svolgimento e le competenze della procedura di *audit*, per la verifica del rispetto delle norme armonizzate sulla sicurezza dei prodotti e dei requisiti del capo II del regolamento stesso. Il procedimento distingue le ipotesi di un controllo interno da uno esterno affidato a un organismo notificato. In ragione dell'attuale esperienza dei certificatori professionali limitata alla sicurezza dei prodotti, per le IA non collegate ai prodotti di regola la valutazione di conformità è operata dallo stesso fornitore. Diversamente l'atto specifica che quando il sistema è destinato ad essere messo al servizio dalle autorità in materia di immigrazione o di asilo l'attività di *audit* dovrà essere svolta dall'autorità di vigilanza del mercato. Vi sono poi altre due elementi che meritano di essere segnalati: la registrazione nella banca dati UE per i sistemi di IA ad alto rischio in questo settore (nello specifico poligrafi; sistemi che valutano rischio di immigrazione irregolare e sistemi che assistono le autorità pubbliche nella nell'esame delle domande di asilo, di visto o di permesso di soggiorno e per i relativi reclami) avviene in una sezione non pubblica sicura e comprende solo alcune informazioni; la designazione del

[60] A tal proposito utile è ricordare che «con l'affermarsi delle democrazie conflittuali del Novecento la tecnica finisce per assumere un carattere strumentale perdendo l'aurea della sua piena razionalità», così G. Azzariti, *Tecnica, politica, Costituzione. Perché non solo la politica ma anche la tecnica deve essere limitata dalla Costituzione*, in *Il Governo tra tecnica e politica. Atti del Seminario annuale dell'associazione "Gruppo di Pisa". Como, 20 novembre 2015*, Napoli, 2016, 120.

[61] C. Dumbrava, *Artificial intelligence at EU borders. Overview of applications and key issues*, European Parliamentary Research Service, 2022.

[62] A. Szwed, *The use of artificial intelligence in migration-related procedures in the European Union - opportunities and threats. The use of artificial intelligence in migration-related pro*, in *Procedia Computer Science*, 207 (2022), 3639 ss; H. Beirens, *Rebooting the Asylum System? The Role of Digital Tools in International Protection*, Migration Policy Institute, 2022, all'url: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2022-11/mpi_digitalization-asylum_final.pdf; M. Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, in *BioLaw Journal –Rivista di BioDiritto*, 2, 2021, 433 ss.

Garante per la protezione dei dati personali come autorità di vigilanza del mercato (art. 74, par. 8). Entrambe le disposizioni costituiscono delle eccezioni al sistema di registrazione e di *governance* come disegnato, rispettivamente, agli artt. 49 e 70 del regolamento.
Andando alla categorizzazione del rischio, il regolamento premette che le persone migranti si trovano spesso in una posizione particolarmente vulnerabile e il loro futuro dipende dall'esito delle azioni delle autorità pubbliche competenti (cons. 60). Così, nella *Proposta* formulata ad aprile 2021, l'AI Act ha classificato come ad alto rischio i sistemi di IA impiegati nei settori dell'immigrazione e dell'asilo. Nessuno dei sistemi, nella prima formulazione della *Proposta*, era considerato a rischio inaccettabile, mentre nell'alto rischio rientravano (par. 7 dell'allegato III):
a) i poligrafi e gli strumenti analoghi, per rilevare lo stato emotivo di una persona fisica;
b) i sistemi per valutare un rischio per la sicurezza, l'immigrazione irregolare e la salute, di chi intende entrare o ha già fatto ingresso nel territorio di uno Stato membro;
c) i sistemi di verifica dell'autenticità dei documenti di viaggio e dei documenti giustificativi delle persone fisiche e per individuare i documenti non autentici mediante il controllo delle caratteristiche di sicurezza;
d) i sistemi di IA destinati ad assistere l'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami.
In seguito agli emendamenti del Parlamento, il quadro dei rischi possibili ha subito tre importanti cambiamenti, il primo dei quali ha riguardato specificamente l'immigrazione, mentre gli altri due hanno verosimilmente ricadute in tale ambito: 1) il passaggio dei sistemi di rilevamento delle emozioni nella gestione delle frontiere dall'alto rischio al divieto (art. 5, par. 1, lett. *d-quater)*; 2) la soppressione delle eccezioni al divieto di identificazione biometrica da remoto in tempo reale in spazi accessibili al pubblico, per le ipotesi della prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico (art. 5, par. 1, lett. *d-ii)*; 3) il divieto dell'analisi di filmati registrati di spazi accessibili al pubblico attraverso sistemi di identificazione biometrica remota «a posteriori», salvo la previa autorizzazione giudiziaria (art. 5, par. 1, lett. *d-quinquies*).
Tra le ipotesi di IA ad alto rischio sono state aggiunte nell'allegato III, punto 7, lett. *d-bis* e *ter* i sistemi impiegati per monitorare, sorvegliare o elaborare dati nel contesto delle attività di gestione delle frontiere allo scopo di individuare, riconoscere o identificare persone fisiche; infine, quelli per prevedere o anticipare le tendenze relative ai movimenti migratori e all'attraversamento delle frontiere.
Tale schematizzazione ha ricevuto nuovi emendamenti a seguito dall'accordo raggiunto il 9 dicembre 2023. In particolare, si nota l'eliminazione: del divieto di usare sistemi di riconoscimento emotivo alle frontiere[63]; del divieto assoluto dei sistemi di IA di riconoscimento e identificazione biometrica «in tempo reale» e «a posteriori» negli spazi accessibili al pubblico; del divieto di categorizzazione biometrica; dei sistemi per la verifica dell'autenticità dei documenti di viaggio e rilevamento di documenti non autentici, controllandone le caratteristiche di sicurezza dall'elenco delle IA ad alto rischio. Inoltre, i fornitori dei sistemi ad alto rischio potranno adottare la cd. *filter provision* (art. 6, par. *2-bis*), auto-dichiarando che la macchina non costituisce un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali, quando il sistema di IA sia destinato a svolgere un compito procedurale ristretto; o a non modificare la valutazione umana; o a svolgere compiti

[63] European Parliament, *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*, Press Releases IMCO LIBE, 9-12-2023; Council of the EU, *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, Press release, 9-12-2023; European Commission, *Commission welcomes political agreement on Artificial Intelligence Act*, Press release, 9-12-2023.

preparatori. Un intervento modificatore che aprirà il varco alla fuga dei sistemi dal cd. rischio ridotto con facili esiti elusivi degli artt. 10-15 dell'*AI Act*[64]. A ciò si aggiunge l'eliminazione della garanzia prevista per i sistemi di IA ad alto rischio nell'ultimo paragrafo dell'art. 14 sul controllo umano, che predispone una doppia verifica dell'*output*: precisamente nessuna azione o decisione è presa dall'utente-impiegato sulla base dell'*output*, a meno che questa non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità. La doppia verifica è stata espunta per le IA ad alto rischio utilizzate a fini di applicazione della legge, migrazione, controllo delle frontiere o asilo, nei casi in cui il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito.

Quanto ai sistemi ad alto rischio sono rimaste inalterate le ipotesi elencate alle lett. *a)* e *b)* e *d)*. Dall'elenco sono state espunte quei sistemi introdotti dagli emendamenti del Parlamento europeo; sono stati invece aggiunti i sistemi di IA destinati a essere usati al fine di individuare, riconoscere o identificare persone fisiche, a eccezione della verifica dei documenti di viaggio.
Dopo avere descritta la modalità con cui l'atto europeo intende affrontare i rischi connessi ai fenomeni migratori, è utile soffermarsi su due profili critici[65].
Il primo riguarda la categorizzazione del rischio: nonostante sia lo stesso considerando 60 dell'*AI Act* a porre l'accento sulla necessità che nel contesto migratorio siano adoperati sistemi di IA che garantiscano l'accuratezza, la natura non discriminatoria e la trasparenza dei risultati, molti sistemi in uso verrebbero in realtà lasciati fuori dell'impianto precauzionale (*infra* par. 2). Tra di essi[66], temporaneamente fino al 2030, le componenti IA dei sistemi di gestione sistemi informatici integrati su larga scala, con ritardo all'adattamento di quattro anni di ritardo rispetto agli altri sistemi ad alto rischio. Si tratta invero di un settore denso di ricadute sui diritti connessi alla protezione dei dati personali, visto che il sistema di interoperabilità – costruito dai regolamenti 817/2019 e 818/2019 – pone sistematicamente sotto stress il principio della limitazione delle finalità del trattamento dei dati (art. 5, lett. *b)*, reg. 679/2016). Basti considerare che l'agenzia Europea competente, EU-Lisa, ha la gestione operativa del sistema d'informazione Schengen, del sistema di informazione visti e del sistema europeo per il confronto delle impronte digitali dei richiedenti asilo, che contribuiscono alla sicurezza dello spazio Schengen[67].
Fuori dall'area dell'alto rischio sono i sistemi predittivi dei movimenti di immigrazione e quelli di sorveglianza delle frontiere, nonostante i rischi significativi connessi ai danni ai diritti fondamentali siano altamente probabili e gravi. A tal proposito, si pensi che i sistemi predittivi dei flussi migratori possono suggerire alle istituzioni nazionali ed europee competenti l'attivazione di strumenti emergenziali nella gestione di afflussi massicci di cittadini stranieri; mentre i sistemi di sorveglianza possono supportare pratiche illegittime come quelle delle espulsioni collettive e la violazione del principio di non respingimento.

---

[64] P. Friedl, G. Gil Gasiola, *Examining the EU's Artificial Intelligence Act*, in *Verfassungsblog*, 7 febbraio 2024.
[65] In tema, N. Vavoula, *Unpacking The Eu Proposal For An Ai Act: Implications For Ai Systems Used In The Context Of Migration, Asylum And Border Control Management*, in *TPQ*, 4, 2022, 119 ss; EDRI, *Uses of AI in migration and border control: A fundamental rights approach to the Artificial Intelligence Act*, 2022, in https://edri.org/wp-content/uploads/2022/05/Migration_2-pager-02052022-for-online.pdf.
[66] Per un'analisi approfondita J. Kilpatrick, C. Jones, *A clear and present danger. Missing safeguards on migration and asylum in the EU's AI Act*, Statewatch, May 2022 e N. Vavoula, *Tr-Ai-Nsforming Migration, Asylum and Border Management in the EU: The Roles of the Ai Act, Interoperable Large-Scale it Systems and EU Migration Agencies,* 2024, disponibile su SSRN: https://ssrn.com/abstract=4765470 or http://dx.doi.org/10.2139/ssrn.4765470.
[67] In tema European Data Protection Supervisior, *Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments*, 23 ottobre 2023, 8-9.

Simili problematicità riguardano anche IA come Centaur[68], un sistema digitale integrato di gestione della sicurezza e l'impiego di algoritmi per l'analisi del comportamento, adoperati nelle isole dell'egeo nelle aree *hotspot*.
Le esclusioni qui brevemente ripercorse sono criticabili se confrontate con gli artt. 1 e 7 dell'*AI Act*, nei quali si specifica che l'IA è da classificare ad alto rischio quando possa impattare negativamente sui diritti fondamentali.
Recentemente la Corte di giustizia ha chiarito che le limitazioni nel trattamento dei dati, seppure si svolgano nel rispetto del principio di legalità e proporzionalità «comportano ingerenze nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta [dei diritti fondamentali dell'Unione europea]»[69]. Da ciò ne dovrebbe allora derivare un'indicazione di metodo per il legislatore europeo: tutti quei sistemi che adoperano dati biometrici e personali eccedendo quanto indicato nei principi dell'art. 5, reg. 679/2016, dovrebbero per ciò solo rientrare nell'allegato III.
Quanto appena indicato mette in luce un uso poco attento della categoria dei diritti fondamentali all'interno dell'*AI Act*. Accogliendo la nozione di «fondamentalità» secondo un'accezione di gerarchia materiale e assiologica[70], il legislatore europeo da un lato sembra non considerare il catalogo dei diritti del suo stesso ordinamento (artt. 7 e 8 Carta dei diritti fondamentali) per la categorizzazione del rischio, dall'altro il bilanciamento tra l'innovazione e protezione dei diritti fondamentali non segue sempre i canoni della proporzionalità, ragionevolezza e necessarietà[71].
Un altro interrogativo che emergerà dall'implementazione del futuro regolamento è se esso riuscirà a garantire effettivamente il diritto a contestare le decisioni algoritmiche[72] o se invece rafforzerà la tendenza di chi utilizza un'IA all'*automation bias*, cioè a essere catturati dall'*output* della macchina. Questo rappresenterà evidentemente un aspetto cruciale per la garanzia dei diritti fondamentali, ma che giocoforza sfugge alla forza coercitiva del diritto. La proposta di regolamento cerca di rafforzare tale piano con l'elenco di diritti dell'art. 50 e di rimedi davanti ad un'autorità indipendente e/o giudiziaria di cui agli artt. 85 e 86[73], che emulano il diritto alla *meaningful information about the logic involved* dei sistemi automatizzati, ex art. 22 reg. 679/2016.
È quindi ancora prematuro stabilire se la costruzione di algoritmi orientati dal Libro Bianco sarà in grado di replicare il bilanciamento tra accoglienza/esclusione dello straniero che incombe ad ogni ordinamento individuare, senza eludere al contempo gli obblighi nazionali, internazionali e dell'Unione europea relativi al diritto di asilo, nonché quelli derivanti dall'applicazione del principio di non respingimento.

---

[68] C. Petridi, *Greek camps for asylum seekers to introduce partly automated surveillance systems*, in *Algorithm Watch*, all'url: https://algorithmwatch.org/en/greek-camps-surveillance/
[69] CGUE, 21 giugno 2022, *Ligue des droits humains*, §231.
[70] Su tutti G. Pino, *Diritti e interpretazione. Il ragionamento giuridico nello Stato costituzionale*, Bologna, 2010, 98.
[71] In tema si veda anche il testo di N. Smuha et alii, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, August 5, 2021, url: https://ssrn.com/abstract=3899991, spec. 9 ss., ove si aggiunge un'altra considerazione che pure merita di essere considerata. Le basi giuridiche dell'AI Act, l'art. 114 e l'art. 16 TFUE, che guidano rispettivamente l'armonizzazione delle regole per il funzionamento del mercato interno e della protezione dei dati «creates an uneasy marriage that does not provide protection for the full gambit of potential interferences, intrusions and violations of fundamental rights made possible by the development, deployment and use of AI systems in the EU» (pp. 10-11).
[72] Sugli aspetti sostanziali e procedurali già vigenti e quelli che invece potrebbero ispirare la nascita di un vero e proprio *right to contest AI* si veda M.E. Kaminski, J.M. Urban, *The Right to Contest AI,* in *Columbia Law Review,* 7, 2021, 1957 ss., *passim.*
[73] Sul catalogo dei diritti nell'AI Act v. G. De Minico, *Giustizia e intelligenza artificiale: un equilibrio mutevole,* in *Rivista AIC*, 2, 2024, 92.

4. Il rilevamento delle emozioni alle frontiere: AI Act e diritti neuronali. Tra gli impieghi critici dell'IA alle frontiere rientrano i sistemi di rilevamento delle emozioni, ossia quelle tecnologie che si propongono di analizzare espressioni facciali, movimenti del corpo, tono della voce e dati biometrici per misurare o dedurre le emozioni della persona[74], tant'è che l'evoluzione delle applicazioni biometriche si sta integrando sempre di più coi sistemi di riconoscimento emotivo, nei luoghi in cui il riconoscimento facciale è già in uso[75].

Il campo del riconoscimento emotivo è denso di questioni anzitutto di carattere etico-filosofico, ove si consideri che per la scienza la risposta alla domanda su cosa sia un'emozione è aperta[76], ma anche per il settore ingegneristico, stante la difficile traduzione nella modellistica matematica di software di codificazione emotiva[77].

Nei sistemi di intelligenza artificiale cd. emotivi la capacità computazionale decifra uno spazio intimo e riservato per lo più a studi clinico-psicologici. La combinazione tra la tecnologia del riconoscimento parziale (*Facial Emotion Recognition*, d'ora innanzi FER) e l'intelligenza artificiale ha dato vita a sistemi attualmente molto in uso nei settori del *marketing* e della vendita, nei *device* associati dell'*Internet of Things*, ma anche per usi polizieschi.

Le analisi svolte dalle FER si compongono di tre fasi: il rilevamento del volto, dell'espressione facciale, e, infine, la classificazione dell'espressione in uno stato emotivo, svolta dall'algoritmo. Quando le FER sono impiegate insieme a strumenti di identificazione biometrica, lo scopo è andare oltre la biometria. Tale è proprio il caso dei poligrafi sperimentati ai valichi di frontiera di Ungheria, Grecia e Lettonia, per il rilevamento dell'inganno e la previsione del rischio con *iBorderCtrl*[78], un sistema di IA che mira a valutare un rischio per la sicurezza, di immigrazione irregolare o per la salute pubblica, rappresentato da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro. Esso ha replicato la versione statunitense dell'*Automated Virtual Agent for Truth Assessment in Real-time* (AVATAR), dove un agente automatizzato adatta la sua attività di conversazione all'interlocutore, con il quale svolge interviste brevi in una serie di contesti di *screening*, come domande di pre-assunzione, rilascio del visto di ingressi e altri scenari che comportano valutazioni di credibilità. Durante l'interazione vengono identificati quei comportamenti sospetti o irregolari che meritano ulteriori indagini[79].

Applicando tale tecnologia al contesto delle frontiere, questa forma di *screening* pre-arrivo automatizzato si propone di ridurre la quantità di tempo per lo svolgimento dei controlli di sicurezza riguardanti il cittadino straniero. Il migrante è quindi sottoposto all'intervista di un *avatar*, che identificherà i cd. «biomarcatori di inganno» verbali e non verbali, come microespressioni facciali associate alla menzogna (ad. es. l'ammiccamento dell'occhio sinistro, l'aumento del rossore del viso, il movimento della testa). Inoltre, nello sviluppo di

---

[74] J. Buolamwini, V. Ordóñez, J. Morgenstern, E. Learned-Miller, *Facial Recognition Technologies: A Primer*, 2020, 4-5.

[75] European Parliamentary Research Service, *Regulating facial recognition in the EU*, 2021, 4.

[76] Per una ricostruzione delle diverse posizioni G. Sacco, *Che cos''e un'emozione? Una domanda senza (possibile) risposta?*, in *Sistemi intelligenti*, 2, 2021, 319 ss.

[77] D. White, H. Katsuno, *Artificial emotional intelligence beyond East and West*, in *Internet Policy Review*, 1, 2022, 7 ss.

[78] European Commission, Smart lie-detection system to tighten EU's busy borders, all'url: https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders.

In tema: J. Sánchez-Monedero, Lina Dencik, *The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl, Information*, in *Communication & Society*, 25, 3, 2022, 413-430; L. Hall, W. Clapton, *Programming the machine: gender, race, sexuality, AI, and the construction of credibility and deceit at the border*, in *Internet Policy Review* 4, 2021.

[79] National Center for Border Security and Immigration, *Appraising the AVATAR for Automated Border Control Results of a European Union Field Test of the AVATAR System for Interviewing and Passport Control*, 2014.

iBorderCtrl sono stati unificati diversi moduli per accelerare la procedura di attraversamento dei confini, che consentono simultaneamente di rilevare dati biometrici, verificare i documenti di viaggio, correlare i database esterni (come il SIS), svolgere la corrispondenza dei volti e valutare del rischio prima ancora che il viaggiatore arrivi alla frontiera. Tutte le informazioni così raccolte sono a disposizione degli agenti di frontiera, per lo svolgimento del controllo effettivo.

L'impiego di tali sistemi è stato fortemente criticato per tre aspetti: a) la fallacia dei suoi presupposti, ossia ritenere fondata la teoria secondo cui mentire è un compito emotivamente impegnativo, che lascia sempre tracce comportamentali non verbali[80], che corrispondono a un insieme di emozioni pre-definite. A ciò si aggiunga il problema della capacità di «leggere» la verità anche nella comunicazione interculturale, ponendo specifiche questioni in termini di giustizia dei dati per l'addestramento dell'IA[81]; b) l'assenza di trasparenza, data dal mancato accesso ai documenti riguardanti l'autorizzazione del progetto *iBorderCtrl* (compresa la valutazione etica e giuridica degli strumenti, delle componenti tecniche e dei metodi sviluppati nel progetto).

Nonostante l'eurodeputato Patrick Breyer avesse chiesto all'Agenzia esecutiva europea per la ricerca di potervi accedere, invocando il diritto della collettività a conoscere quando lo sviluppo di un progetto comporti ingerenze non etiche o illegittime nel diritto al rispetto della vita privata dei cittadini, per consentire un dibattito pubblico e democratico informato sull'introduzione di nuovi sistemi di controllo di massa controversi, il Tribunale dell'Unione[82] ha ritenuto equo il bilanciamento tra il diritto a essere informati e la tutela degli interessi commerciali della società sviluppatrice, attraverso la diffusione dei risultati della ricerca con pubblicazioni scientifiche; c) l'accuratezza dei risultati, giacché dalla sperimentazione sono stati raggiunti tassi di veridicità dei risultati bassi (che si attestano intorno al 73-75%[83]), con il rischio di non essere adeguatamente compensati dal successivo intervento umano, anche a causa dell'*automation bias*[84].

Con gli emendamenti proposti dal Parlamento europeo all'AI Act, il legislatore europeo sembrava aver accolto le preoccupazioni in merito alla base scientifica dei sistemi di IA volti a rilevare le emozioni e alla loro variabilità in base alle culture, alle situazioni e persino in relazione a una stessa persona[85]. L'inaffidabilità e, di conseguenza, i gravi rischi di abuso hanno portato il Parlamento europeo a vietare l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati in tali contesti per rilevare lo stato emotivo delle persone fisiche alle frontiere (art. 5, par. 1, lett. *d-quater*). Non priva di confusione era però la scelta di non vietare in blocco questi sistemi, ma di consentirne l'uso per l'identificazione delle persone fisiche, attraverso sistemi di IA utilizzati per trarre conclusioni sulle caratteristiche personali delle persone fisiche sulla base di dati biometrici o basati su

[80] P. Ekman, E.L. Rosenberg, *What the face reveals: Basic and applied studies of spontaneous expression using the facial Action Coding system (FACS),* 2nd ed., Oxford, 2005.

[81] J. Sánchez-Monedero, Lina Dencik, op. cit., 421.

[82] Tribunale UE, 15 dicembre 2021, *Breyer c. REA*, causa T-158/19.

[83] C. Dumbrava, Op. cit., 17.

[84] Su cui da ultimo L. Gugliotta, A. Elbi, *Will AI 'subtly' take over decision-making in the EU migration context? Warnings and lessons from ETIAS and VIS*, in *2023 EULEN Conference on AI Systems and Enforcement: Between Effectiveness and the Rule of Law*, 14, all'url: https://jmn-eulen.nl/wp-content/uploads/sites/575/2023/03/5.3.-Gugliotta-Elbi.-.pdf

[85] Il cons. 26 quater rileva infatti tra le principali carenze di tali tecnologie: la limitata affidabilità (le categorie di emozioni non sono espresse in modo affidabile attraverso un insieme comune di movimenti fisici o fisiologici né associate in modo inequivocabile agli stessi), la mancanza di specificità (le espressioni fisiche o fisiologiche non corrispondono perfettamente alle categorie di emozioni) e la limitata generalizzabilità (gli effetti del contesto e della cultura non sono sufficientemente presi in considerazione).

elementi biometrici (All. III, punto 1. lett. *a-bis)*).
Come anticipato, il divieto di impiegare tali sistemi alle frontiere non è sopravvissuto alla fase dei triloghi; pertanto, i poligrafi potranno essere immessi nel mercato, al pari dei sistemi di identificazione e categorizzazione biometrica, inseriti entrambi tra le IA ad alto rischio.
Le censure sollevate nel contesto delle migrazioni sono particolarmente criticabili, considerato che gli esiti della decisione algoritmica «*can be life-changing*»[86]. Il rilevamento emotivo non accurato o errato, che non sia compensato dall'autonomia dell'intervento umano che lo corregga, oltre a doversi valutare criticamente rispetto all'art. 22, reg. 679/2016, alle frontiere potrebbe generare ulteriori conseguenze, più gravi della mancata protezione dei dati neurali alle condizioni date dall'art. 9, reg. 679/2016, perché suscettibile di violare il diritto a non subire il respingimento alla frontiera (riconosciuto a chiunque la attraversi) e il diritto al riconoscimento dello status di rifugiato (per i richiedenti asilo).
Oltre ai tre aspetti critici ben evidenziati, sembra di vederne uno ulteriore: il *vulnus* ai neurodiritti.
Tale emergente categoria si propone di proteggere la *privacy* della mente[87] dalle interferenze delle neuroscienze e delle neurotecnologie, per la tutela della libertà cognitiva. Con questa espressione si intende il controllo che ogni persona ha con lo sviluppo del proprio processo mentale interno[88], ossia il diritto «*to mental self-determination guarantees individuals sovereignty over their minds*»[89].
In tal senso i biomarcatori dell'inganno alle frontiere non sono differenti dalle tecnologie della risonanza magnetica funzionale (fMRI) impiegate nel processo penale come macchine della verità.
La crescente dipendenza da strumenti che promettono la rivelazione di verità «oggettiva»[90] minaccia la libertà morale e l'autonomia individuale, in quanto questi potrebbero influenzare la capacità di mantenere il controllo sulla sfera più intima della propria esistenza: la mente[91] e il pensiero nella sua quintessenza, prima che si verifichi la sua manifestazione all'esterno[92].
Mentre la questione sulla validità e l'ammissibilità delle prove nel processo penale, tramite strumenti che realizzano una connessione diretta con il cervello e dunque con gli stati mentali, è oggetto di attenzione giurisprudenziale e riflessione dottrinale – data invero dalla presenza di una precisa indicazione legislativa (l'art. 188 c.p.p. rubricato «Libertà morale della persona nell'assunzione della prova») – le implicazioni sull'uso della forza in altri contesti,

[86] IOM, *World Migration Report 2022: Chapter 11 - Artificial intelligence, migration and mobility: implications for policy and practice*, 16.
[87] La privacy della mente «*denotes the domain of a person's active brain processes and experiences – perceptions, thoughts, emotions, volition; roughly corresponding to Kant's notion of the locus internus in philosophy – which are exceptionally hard (if not impossible) to access externally*», così P. Kellmeyer, *'Neurorights': A Human Rights–Based Approach for Governing Neurotechnologies*, in S. Voeneky, P Kellmeyer, O. Mueller, W. Burgard (a cura di), *The Cambridge Handbook of Responsible Artificial Intelligence. Interdisciplinary perspectives*, Cambridge University Press, 2022, 414.
[88] M. Ienca, *On Artificial Intelligence and Manipulation*, in *Topoi*, vol. 42, 2023, 838.
[89] J.-C. Bublitz, *My Mind is Mine!? Cognitive Liberty as a Legal Concept*, in E. Hildt, A. Francke (a cura di), *Cognitive Enhancement*, Cham, 2013, 242.
[90] A. Bonomi, *Libertà morale ed accertamenti neuroscientifici: profili costituzionali*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2017, 140, parla di contemporaneo metodo socratico maieutico di «tirare fuori» la verità.
[91] «[…] it is clear that what was historically understood as the «mind» is a product of brain activity. This activity includes all your thoughts, your memories, your imagination, your decisions, your behaviour, and your emotions. As such, the brain is inextricably linked with human identity», così R. Yuste, T. de la Quadra-Salcedo, *Neuro-Rights and New Charts of Digital Rights: A Dialogue beyond the Limits of the Law*, in *Indiana Journal of Global Legal Studies*, 1, 2023, 21.
[92] M. Ienca, R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences, Society and Policy*, 5, 2017, 22; G. De Minico, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, in *Federalismi.it*, 6/2024, 5 ss.

come quello delle migrazioni o nel settore lavoristico, non sono state messe ugualmente a fuoco. Eppure, lo stanziamento di risorse in progetti di poligrafi[93] lascia intendere che il futuro sviluppo della gestione delle frontiere Schengen si realizzerà anche attraverso l'IA di tipo emotivo. È verosimile dunque attendersi che sempre più l'ordinamento sarà chiamato a riflettere sui neurodiritti dello straniero.

Esaurire le questioni aperte dalla libertà cognitiva non è semplice, poiché entrano in discussione temi complessi che vanno dall'emersione di una quarta generazione dei diritti[94], al tono costituzionale dei neurodiritti e a come inglobare la tutela della libertà morale nell'art. 13 Cost., in assenza di attività inibitorie all'autodeterminazione. L'impiego delle neurotecnologie può essere infatti sia di mera registrazione, sia di alterazione delle attività neuronali (il rilevamento emotivo alle frontiere rientra nella prima delle due ipotesi indicate). Ciò comporta che la libertà cognitiva sia da intendere come concetto multidimensionale, che per taluni rappresenta il sostrato di ogni altra libertà[95], per altri coinciderebbe con la sfera dell'autodeterminazione mentale[96], mentre altri studiosi ancora notano il suo fondamento nella *neuroprivacy*[97]. Tre letture differenti che aprono alla massima tutela dei diritti, o viceversa a ipotesi più restrittive, le quali proteggono dalle intrusioni nella sfera della libertà solo quando la tecnologia è in grado di alterare fisicamente o psichicamente il comportamento della persona.

Lo scudo protettivo dell'art. 13 Cost. è usato con cautela dalla Corte costituzionale[98]. Quest'ultima avverte sì l'esigenza di allargarne la portata «non soltanto innanzi allo spiegamento di forme coercitive (il cui esercizio segna la più icastica manifestazione del monopolio statale della forza)», ma anche per quei casi di degradazione giuridica che incidono sulla pari dignità della persona, tuttavia, non ogni mortificazione della sfera morale ricade nel nucleo protettivo dell'*habeas corpus*. Si dovrebbe allora ricavarne che quando l'obiettivo del mezzo tecnologico sia di alterazione dell'attività delle mente si entri nel nucleo della libertà personale, quando invece l'obiettivo sia di mera registrazione in quello della privacy.

Quest'ultima, nella sua originaria aspirazione, è data dal riconoscimento da parte dell'ordinamento a ciascun individuo di una chiusura allo sguardo altrui: «*the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others*»,[99] mentre, negli sviluppi successivi, ha finito per affermarsi prima come tutela della riservatezza alla protezione dei dati personali e poi come autodeterminazione informativa[100].

La vita privata non trova in Costituzione una norma esplicita che predisponga un sistema di garanzie: esse sono mutevoli, in relazione al contesto di cui si discorre, pur trovando nell'art. 2 (principio personalista) e nell'art. 3 (pieno sviluppo della persona umana) il proprio

---

[93] Statewatch, *L'UE ha speso oltre 340 milioni di euro per la tecnologia AI di frontiera che la nuova legge non riesce a regolamentare*, maggio 2022.

[94] A. Iannuzzi, F. Laviola, *I diritti fondamentali nella transizione digitale*, in *Diritto costituzionale, Diritti di libertà e nuove tecnologie fra libertà e uguaglianza*, 1, 2023, 10.

[95] W. Sententia, *Neuroethical Considerations: Cognitive Liberty and Converging Technologies for Improving Human Cognition*, in *Annals of the New York Academy of Sciences*, 1, 2004, 221-228; N.A. Farahany, *Incriminating Thoughts*, in *Stanford Law Review*, 2012, 407.

[96] J.-C. Bublitz, op. cit., 234.

[97] Ossia «lo spazio inviolabile della persona nei confronti di qualsiasi ingerenza indebita, sia essa un'estrazione informativa o una interferenza attiva, richiamando il livello neurale in un approccio metodologicamente riduzionista, ancorché non per questo riduttivo: è la dimensione del corpo il punto di partenza e di arrivo dei diritti, delle libertà, dell'autodeterminazione, della dignità», così F. Cirillo, *Neurodiritti: ambiguità della "libertà cognitiva" e prospettive di tutela*, in *Consulta Online*, 2, 2023, 704.

[98] *Ex multis*: sentenze n. 68/1964, n. 419/1994 e n. 127/2022.

[99] Su tutti Warren e Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 5, 1890, 199.

[100] M.F. De Tullio, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 4, 2016, 652 ss.

architrave concettuale di sostegno.
Tali riflessioni recano con sé nuovi dubbi che l'operatore giuridico che si muova alla luce della Costituzione (il legislatore, l'interprete e i funzionari ai valichi di frontiera) è chiamato a risolvere: identificare gli interessi in conflitto, riconducendoli ai valori costituzionali coinvolti, e orientare il verso delle operazioni di bilanciamento, tenendo conto dell'impostazione personalistica.
Tra i temi più urgenti rientra l'identificazione dell'ambito protettivo in cui ricadono i bisogni scaturenti dall'invasione della mente da parte della tecnologia; la titolarità dei neurodiritti e la posizione – paritaria o meno – degli stranieri rispetto a essi. Va in particolare definito se le esigenze di mantenimento dell'ordine pubblico e della sicurezza, ma anche di protezione del principio di non respingimento da parte delle autorità ai valichi di frontiera, giustifichino trattamenti differenziati tra cittadino e straniero nella protezione della libertà «da» intrusioni esterne alla propria sfera mentale, emozioni e dati neurali. Se la risposta sarà affermativa, occorrerà chiarire quali e quante informazioni mentali e dati neurali possano essere nella disponibilità degli attori pubblici e infine a quali condizioni.
A ben vedere si tratta di questioni per le quali l'*AI Act* e il reg. 679/2016 possono offrire una tutela apprezzabile, ma che non è in grado di esaurire in modo convincente la complessità delle questioni aperte. È allora urgente che il legislatore si misuri con le nuove dimensioni dei problemi costituzionali della libertà e dell'eguaglianza[101] incisi e riconfigurati dal contesto storico-ambientale descritto (*infra* § 2).
La definizione delle questioni della giustificazione, della struttura e del contenuto di tali processi[102] appaiono prioritari rispetto alle questioni della sicurezza dell'IA impiegata, delle regole sull'affidabilità del rilevamento emotivo da parte dell'algoritmo, della capacità di «leggere» la verità nella comunicazione interculturale, in relazione alle migrazioni forzate[103] e, infine, del rafforzamento del consenso al trattamento dei dati[104].

5. Considerazioni finali. I temi indagati attraversano i settori della tecnologia e dell'immigrazione, mettendo in luce il doppio binario – inclusione e competizione – verso cui è orientato l'utilizzo delle nuove tecnologie nella disciplina giuridica dell'intelligenza artificiale. Non è un caso che a distanza di un giorno l'uno dall'altro, nei messaggi di fine e inizio anno[105], il nostro Presidente della Repubblica e il Papa abbiano pronunciato parole importanti sul progresso tecnologico dell'intelligenza artificiale, mettendo in guardia dai pericoli, tra i quali su tutti la crescita delle diseguaglianze e la perdita di senso del limite e additato le stelle polari che devono invece guidarne lo sviluppo, su tutte la dignità della persona e la ricerca della pace.
Come visto, l'AI Act alimenta sia il versante antropocentrico, sia quello competitivo attraverso una legge pioneristica che ha un obiettivo ambizioso: rendere sicuro il mercato dell'intelligenza artificiale. Con l'analisi svolta si è cercato di segnalare i punti di forza e i limiti.

---

[101] A. D'Aloia, *Eguaglianza. Paradigmi e adattamenti di un principio 'sconfinato'*, in *Rivista AIC*, 4, 2021, spec. 92-93.
[102] F. Cirillo, *Neurodiritti: ambiguità della "libertà cognitiva" e prospettive di tutela*.
[103] Ulteriori preoccupazioni etiche su iBorderCtrl sono avanzate da P. Molnar, *Emerging voices: Immigration, iris-scanning and iBorderCTRL – The human rights impacts of technological experiments in migration*, in *OpinioJuris*, 2019, sulla capacità dell'algoritmo di non può tenere conto del trauma e dei suoi effetti sulla memoria, o delle differenze culturali nella comunicazione; sulla condivisione delle informazioni senza il consenso delle persone, nonché sui pregiudizi nell'identificazione attraverso il riconoscimento facciale, poiché le tecnologie di riconoscimento facciale fanno fatica ad analizzare le donne o le persone con tonalità della pelle più scure.
[104] G. Scorza, *Neuroverso. Il cervello è nudo. Quale impatto sulle nostre vite, diritti e libertà*, Milano, 2023, cap. 9, 151 ss.
[105] V. esergo.

Nel caso specifico delle migrazioni, si è provato a capire se la loro classificazione come «sistemi ad alto rischio» sia di per sé idonea a evitare l'adozione di decisioni *biased*, che si fondino su una compressione degli artt. 7 e 8 della Carta dei diritti fondamentali e siano produttive di effetti giuridici negativi assai incisivi sulla gestione della mobilità umana. Ne è emersa la preoccupazione di riversare nella categorizzazione ad alto rischio l'idea di una panacea protettiva verso gli utenti-consumatori, visto che taluni sistemi non rientrano nell'allegato III, mentre per quelli che vi rientrano la via di fuga disegnata dall'art. 6, par. 3 appare ampia e generica. A ciò si aggiunga che il sistema degli obblighi non è concretamente definito, ciò induce a dubitare che la presunzione di conformità dell'algoritmo costituzionale possa realizzarsi *by design*. Non in ultimo le titubanze su cosa il regolamento intenda per trasparenza ridonderanno sulla capacità del *deployer* di comprendere l'*output* e sulla concreta reclamabilità della persona interessata. Preoccupazione accresciuta in un contesto come quello delle politiche di immigrazione e di asilo, vista l'elevata presenza di automatismi amministrativi (ad esempio per il rilascio del nulla osta al visto di ingresso) o di procedimenti nei quali le dichiarazioni del richiedente asilo costituiscono la principale fonte di prova da valutare (tipico è il caso della protezione internazionale).

Invero, l'applicazione dell'IA all'ordine sociale pone un dilemma dalle radici più profonde, che tocca il rapporto tra scienza e diritto: la sedicente imparzialità della decisione non umana[106]. All'opposto, la stessa è ineluttabilmente legata alle informazioni che hanno allenato l'IA; ciò induce a domandarsi in che modo possa realizzarsi un algoritmo orientato ai valori e ai principi costituzionali (non solo la non-discriminazione) e se vi sia bisogno di uno *human oversight* rafforzato per l'IA utilizzata dalla pubblica autorità in settori ad alto tasso di politicità, come l'immigrazione e l'asilo.

Quesiti del genere, o altri che potrebbero ancora formularsi, presuppongono l'osservazione delle trasformazioni del contesto storico-ambientale e richiedono nuovi sforzi al progetto del costituzionalismo: rispondere alle nuove istanze di tutela per «coprire l'intero arco delle esigenze dell'uomo/cittadino»[107]. Tra di esse, sembra prioritario assecondare la richiesta costituzionale della riserva di legge[108] quando nel mercato dell'intelligenza artificiale l'utente-consumatore sia consapevolmente o meno chiamato a sacrificare spazi di libertà. Il principio di legalità, che intervenisse in una fase antecedente o comunque concomitante alla regolazione «sulla» tecnica, dovrebbe rappresentare la fonte che esaudisca la commensurabilità tra le manifestazioni delle libertà fondamentali e gli altri interessi in gioco — e perciò suscettibili di compromessi —, vale a dire l'innovazione e la competitività del mercato europeo.

Abstract. Il contributo in oggetto analizza le caratteristiche del regolamento sull'intelligenza artificiale, osservando, attraverso le categorie del costituzionalismo, il sistema di categorizzazione del rischio proposto, le incertezze giuridiche nella definizione legislativa degli obblighi imposti ai fornitori e il catalogo dei diritti degli utenti. Un focus specifico riguarda l'utilizzo di sistemi di intelligenza artificiale nei settori dell'immigrazione e l'asilo e come questi vengono considerati dal futuro regolamento europeo. Infine, il *case study* è sul

[106] A. D'Aloia, *Intelligenza artificiale, società algoritmica, dimensione giuridica. Lavori in corso*, in *Quaderni costituzionali*, 3, 2022, 665; M. Luciani, *La sfida dell'intelligenza artificiale*, in *La lettera: Libertà di ricerca e intelligenza artificiale*, *AIC*, 12, 2023.

[107] R. Nania, op. cit., 4; sulle frontiere della democrazia, diritti e eguaglianza ai tempi dell'intelligenza artificiale A. Patroni Griffi, *Bioetica, diritti e intelligenza artificiale: una relazione ancora da costruire*, in Id. (a cura di), *Bioetica, diritti e intelligenza artificiale,* Milano-Udine, 2023, 10; sulla libertà cognitiva e i prerequisiti sia delle libertà negative che di quelle positive M. Ienca, R. Andorno, op. cit., 11.

[108] Su tutti, G. Amato, *Individuo e autorità nella disciplina della libertà personale*, Milano, 1967, 301 ss.

rilevamento delle emozioni alle frontiere e le questioni giuridiche connesse, alla luce dell'AI Act e dei cosiddetti *neurorights*.

Abstract. The contribution analyzes the characteristics of the regulation on artificial intelligence, observing, through the categories of constitutionalism, the proposed risk categorization system, the legal uncertainties in defining the obligations imposed on providers, and the catalogue of user rights. A specific focus concerns the use of artificial intelligence systems in the immigration and asylum fields and how future European regulation considers these. Finally, the case study deals with emotion detection at borders and the related legal issues in light of the AI Act and the so-called neurorights.

Parole chiave. Costituzionalismo – regolamento sull'intelligenza artificiale – categorizzazione del rischio – rilevamento delle emozioni.

Key words. Constitutionalism – regulation on Artificial Intelligence – risk based approach – immigration and asylum – emotion detection.