La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio

di Barbara Marchetti e Leonardo Parona•

Abstract: *The regulation of artificial intelligence: the United States and the European Union in search of a possible balance* – In light of an analysis of recent regulatory interventions, the article examines how the European Union and the United States are addressing the largely common issues posed by artificial intelligence. The analysis shows the differences between the two regulatory strategies (in terms of objectives, instruments and contents) and inquires the reasons laying behind them. Although moving in disparate directions, regulators on both sides of the Atlantic appear to be in search of a balance between the protection of individual rights and privacy on the one hand, and the promotion of competitiveness and innovation in the field of AI on the other. The article further examines a specific and highly debated use of AI, that is biometric recognition systems.

Keywords: Artificial intelligence; Regulation; United States; European Union; Biometric recognition.

1. Introduzione

La corsa mondiale all'IA e i rapidi avanzamenti che in tema di sviluppo e ricerca sta mostrando la Cina hanno mutato l'assetto geopolitico internazionale, accorciando la distanza tra quest'ultima e gli Stati Uniti[1] e rendendo non più indiscussa la leadership statunitense nello scacchiere della innovazione digitale e tecnologica.

Rispetto ai due principali competitor mondiali, l'Unione europea sta cercando di recuperare terreno, ma appare ancora in ritardo sul fronte della capacità di attrarre investimenti pubblici e privati. La competizione tra i Paesi ha risvolti sul piano della sicurezza nazionale, con chiare implicazioni sul fronte delle scelte regolatorie. Se la regolazione deve certamente andare nella direzione della protezione dei diritti fondamentali e del diritto alla riservatezza, al tempo stesso non deve inibire lo sviluppo e la ricerca dell'IA fissando limiti e regole non sostenibili per gli investitori. Nel contesto

• L'articolo è stato concepito e sviluppato in modo condiviso dagli Autori. Mentre i paragrafi 1 e 4 sono riferibili ad entrambi, i paragrafi da 2 a 2.2 sono attribuibili a Leonardo Parona; i paragrafi da 3 a 3.2 sono attribuibili a Barbara Marchetti

[1] Come enfaticamente asserito dall'ex-Presidente Trump nell'*executive order* 13859 dell'11 febbraio 2019, §1.

statunitense, per esempio, si teme che un ritardo in ricerca e sviluppo dell'IA causato da una regolazione troppo precauzionale possa rendere il Paese più vulnerabile rispetto a possibili attacchi della Cina. Tenere sullo sfondo dell'analisi della regolazione questa tensione competitiva tra gli Stati è necessario per comprendere il contesto più ampio nel quale si collocano le questioni poste dalla regolazione dell'IA.

A proposito di queste ultime, deve in via introduttiva anticiparsi come l'approccio europeo e quello statunitense delineino due modelli regolatori contraddistinti da finalità, strumenti e contenuti differenti. Dal canto suo la Cina appare restia ad introdurre regole che possano ostacolare o rallentare gli avanzamenti tecnologici in nome della tutela dei diritti fondamentali. Al fine di comprendere come Unione europea e Stati Uniti stiano affrontando la regolazione delle questioni – in gran parte comuni – poste dall'IA e quali siano le ragioni che ne sostengono le scelte, nei paragrafi seguenti si offrirà un'analisi dei più recenti interventi regolativi, soffermandoci dapprima sugli atti adottati Oltreoceano e successivamente su quelli proposti dall'Unione europea.

2. L'approccio statunitense alla regolazione dell'intelligenza artificiale

Sono trascorsi poco più di cinque anni da quando, nell'ottobre del 2016, l'amministrazione Obama prese posizione sul futuro dell'intelligenza artificiale[2]; in tale arco di tempo gli investimenti sono cresciuti esponenzialmente[3], le iniziative internazionali di regolazione e cooperazione alla ricerca e allo sviluppo dell'IA si sono moltiplicate[4], l'assetto geopolitico è significativamente mutato. Eppure, il quadro regolamentare statunitense in materia di IA non ha subito trasformazioni profonde. Ciò non significa,

[2] Il riferimento è al report *Preparing for the future of Artificial Intelligence*, pubblicato nell'ottobre del 2016 dal *National Science and Technology Council Committee on Technology* dell'*Executive Office of the President*.

[3] Limitandoci alla spesa federale ed escluso il comparto della difesa, nel 2020 l'amministrazione statunitense ha speso circa un miliardo in IA. Nel 2021 il Congresso ha autorizzato spese in ricerca e sviluppo dell'IA per un miliardo e mezzo (amministrazioni del comparto difesa escluse). Sul punto si veda *AI Intelligence Index Report 2021* curato dall'Università di Stanford (https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf in particolare pp. 17-20). In termini di investimenti, ad aprile 2021 è stato re-introdotto un disegno di legge (*The Endless Frontier Act*) che prevede l'istituzione di un nuovo *Directorate for Technology and Innovation* nell'ambito della *National Science Foundation*, il quale sarebbe autorizzato a spendere 100 miliardi di dollari in ricerca e sviluppo nell'IA nei prossimi 5 anni (sul modello della nota agenzia *DARPA*, la quale opera per il finanziamento di iniziative di ricerca e sperimentazione nel settore della difesa). Contenuti analoghi presenta anche lo *U.S. Innovation and Competition Act* approvato dal Senato (ma non ancora dalla Camera) il 6 agosto 2021.

[4] Sul punto sia consentito rimandare a L. Parona, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici*, soft law *e* self-regulation, in *Rivista della Regolazione dei mercati*, 1, 2020, in particolare 82 ss.

come si vedrà, che la materia non sia stata interessata da iniziative normative; piuttosto, queste ultime non hanno alterato in termini sostanziali il quadro iniziale, sia quanto alle finalità e al contenuto delle medesime, sia quanto alla natura degli strumenti impiegati[5].

2.1. Il quadro normativo e istituzionale

Il percorso intrapreso nell'ultimo biennio dai *rulemakers* statunitensi s'inserisce nel solco tracciato a febbraio 2019 dall'executive order (d'ora in poi e.o.) 13859 *Maintaining American Leadership in Artificial Intelligence*, che ha introdotto la strategia statunitense in materia di intelligenza artificiale, i cui quattro obiettivi principali possono essere sinteticamente ricondotti alla promozione della ricerca e dello sviluppo, alla creazione dei presupposti per una maggiore fiducia dei cittadini nelle applicazioni dell'IA, alla formazione di una forza lavoro competente e capace di trarre beneficio dall'impiego dell'IA, e alla protezione del settore tecnologico statunitense da tentativi di acquisizione e possibili attacchi di *competitors* e Paesi stranieri.

All'interno di tale percorso rilevano sia numerose iniziative di rango legislativo, che tuttavia solo in un numero limitato di casi si sono ad ora effettivamente tradotte in norma di legge, sia alcuni atti dell'Esecutivo, più dettagliati, sebbene non sempre vincolanti. Una terza rilevante categoria è inoltre rappresentata dalle iniziative settoriali di *rulemaking* – più o meno compiute – poste in essere dalle agenzie federali. Di seguito si esamineranno i più rilevanti fra tali interventi normativi, riconducendoli, a fini espositivi, entro categorie per quanto possibile omogenee in termini di contenuto.

Un primo gruppo di iniziative è volto a rafforzare la fiducia dei cittadini nell'impiego dell'IA. Rileva a questo proposito l'e.o. 13960 di dicembre 2020, intitolato *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, il quale ha sinteticamente enunciato alcuni principi di portata generale, in base ai quali l'IA impiegata dalle agenzie federali dev'essere: *lawful and respectful; purposeful and performance-driven; accurate, reliable and effective; safe, secure and resilient; understandable; responsible and traceable; regularly monitored; transparent;* e *accountable*[6]. Parimenti rilevanti sotto questo profilo sono i principi etici adottati dal Dipartimento della Difesa a febbraio 2020, i quali, interessando tanto le operazioni *stricto sensu* militari, quanto quelle *non-combat*, dispongono che i sistemi di IA impiegati dal Dipartimento debbano essere responsabili, giusti (cioè privi di *bias*), tracciabili, affidabili e governabili. Principi sostanzialmente analoghi a quelli appena richiamati sono stati adottati anche dall'*Office of the Director of*

[5] Si veda E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della Regolazione dei mercati*, 1, 2020, 29, nonché, in questo fascicolo, E. Stradella, *Le fonti nel diritto comparato*.
[6] Si veda in particolare la sez. §3 dell'e.o. 13960.

DPCE online
ISSN: 2037-6677

National Intelligence[7]. Più recentemente, il *Government Accountability Office* (di seguito GAO) ha adottato un *accountability framework* con il quale ha inteso declinare tali principi nelle fasi di progettazione, sviluppo, utilizzo e monitoraggio dei sistemi di IA. Tale atto di indirizzo, rivolto sia alle amministrazioni federali, sia al settore privato, si contraddistingue tuttavia per un elevato tasso di genericità ed astrattezza, insistendo ad esempio sulla necessità di assicurare la qualità e la rappresentatività dei dati usati per sviluppare gli algoritmi e sulla predisposizione di – non meglio precisati – meccanismi di monitoraggio sul procedimento e sui risultati. Risulta a questo proposito apprezzabile, nell'ottica della *trustworthy AI*, la coeva pubblicazione da parte del *National Institute of Standards and Technology* (di seguito NIST) di un report volto a identificare e fronteggiare il problema dei *bias* nell'impiego dell'IA. Tale documento dovrebbe auspicabilmente preparare un terreno comune per l'adozione di adeguati standard tecnici e di sicurezza (cui il NIST è istituzionalmente deputato)[8], suggerendo buone prassi da adottare nelle fasi di programmazione, sviluppo e utilizzo dell'IA. Di notevole interesse pare in particolare il tentativo di catalogare le diverse tipologie di *bias*, distinguendo ad esempio tra quelli riguardanti i dati (*data generation bias*, *historical bias*, *inherited bias* e *population bias*) e quelli concernenti l'impiego dell'IA (*amplification bias*, *annotator bias*, *automation complacency* e *loss of situational awareness bias*)[9]. Sempre il NIST, infine, ha pubblicato ad agosto 2020 un report sui *Four Principles of Explainable Artificial Intelligence*, ai sensi del quale gli output dei procedimenti algoritmici dovrebbero essere sempre accompagnati da una spiegazione, la quale dev'essere comprensibile per gli utenti ed accurata, dovendo correttamente riprodurre il procedimento seguito. I sistemi intelligenti dovrebbero inoltre operare solamente secondo i procedimenti programmati ed entro parametri prestabiliti, arrestandosi dinnanzi ai casi per i quali non siano stati progettati o rispetto ai quali gli output presentino livelli di affidabilità inadeguati. Il report non chiarisce, tuttavia, come tali principi possano essere tradotti in concreto in relazione agli algoritmi di *machine learning*.

Una seconda area di intervento riguarda la promozione dell'impiego dell'IA da parte dell'amministrazione federale. L'*Information Technology Modernization Centers of Excellence Program Act*, approvato in via definitiva dal Congresso a dicembre 2020, ha infatti avviato un vasto programma di transizione digitale basato sulla creazione di un centro d'eccellenza sull'IA all'interno della *General Services Administration* (che si occupa dell'approvvigionamento delle amministrazioni federali fungendo, fra le altre cose, da centrale di committenza) e di analoghe strutture all'interno

[7] Il riferimento è ai *Principles of Artificial Intelligence Ethics for the Intelligence Community* e al relativo *Framework*, entrambi adottati il 23 luglio 2020.
[8] Il NIST ha peraltro concluso, a settembre 2021, una consultazione pubblica sulla predisposizione di una *Risk Management Framework* per l'IA, anch'essa funzionale alla predisposizione di standard di sicurezza.
[9] Il report (v. p. 14 ss.) ne individua circa quaranta.

delle *executive agencies*. La legge, che riprende, pur restringendone l'ambito di applicazione, molte delle proposte contenute nell'*AI in Government Act of 2020*[10], delega inoltre il Direttore dell'*Office of Management and Budget* (di seguito OMB) ad adottare atti di *guidance* per l'impiego dell'IA da parte delle agenzie federali e autorizza il Direttore dell'*Office of Personnel Management* ad adottare un piano per l'individuazione delle competenze necessarie alla transizione digitale e all'assunzione di nuovi funzionari dotati di formazione adeguata. Parallelamente, il già ricordato e.o. 13960 ha incaricato il *Federal Chief Information Officers Council* di avviare un processo di catalogazione dei sistemi di IA impiegati dalle agenzie federali[11].

In terzo luogo, solo a gennaio 2021 è stato tradotto in legge il contenuto programmatico della strategia statunitense inaugurata due anni prima con l'e.o. 13859 e, con l'occasione, è andato così consolidandosi un apparato istituzionale frammentario e inizialmente contraddistinto da una certa precarietà – in quanto frutto di atti dell'Esecutivo. Il *National Defense Authorization Act for Fiscal Year 2021*[12] ha a questo proposito istituito il *National AI Initiative Office* e la *National AI Research Resource Task Force*. Il primo, al quale sono attribuite funzioni di impulso e coordinamento, è stato istituito all'interno dell'*Office of Science and Technology Policy* della Casa Bianca[13], nell'ambito del quale operava già l'*Advisory Council on Science and Technology* istituito ad ottobre 2019 dall'e.o. 13895; la seconda, divenuta operativa solo a giugno 2021 con la nomina di dodici esperti provenienti dal settore privato, dall'amministrazione federale e da istituti di ricerca e universitari, è chiamata a svolgere una funzione consultiva a supporto del Presidente e del Congresso[14], predisponendo inoltre una piattaforma – la *National AI Research Resource* – a beneficio di ricercatori e sviluppatori. Quest'ultima, offrendo una raccolta di dati e buone prassi, è volta a promuovere una maggiore diffusione delle competenze necessarie allo sviluppo e all'impiego di sistemi intelligenti.

Non mancano poi proposte di legge più puntuali, le quali affrontano profili specifici o applicazioni settoriali dell'IA. Fra queste ultime si ricordano *in primis*, in materia di sistemi di riconoscimento biometrico, il *Facial Recognition and Biometric Technology Moratorium Act* e il *Commercial Facial Recognition Privacy Act* – dei quali si dirà più approfonditamente nel paragrafo successivo. Risalgono a maggio 2021 due proposte bipartisan

[10] Quest'ultimo è stato approvato solamente dalla Camera il 14 settembre 2020.
[11] Sul punto sia consentito rimandare a L. Parona, "Government by algorithm": *un contributo allo studio del ricorso all'intelligenza artificiale nell'esercizio di funzioni amministrative*, in *Giorn. dir. amm.*, 1, 2021, 10.
[12] La legge, approvata il 1° gennaio 2021, recepisce molti dei contenuti introdotti alla Camera il 12 marzo 2020 con una proposta di legge intitolata *National Artificial Intelligence Initiative Act of 2020*.
[13] La centralità di quest'ultimo – non soltanto in relazione al settore dell'IA – è stata ribadita al Presidente Biden nel memorandum del 27 gennaio 2021, *Restoring Trust in Government through Scientific Integrity and Evidence-based Policymaking*.
[14] È prevista la pubblicazione di due report nel corso del 2022.

concernenti l'impiego di sistemi intelligenti nel comparto *intelligence* e nel settore militare, le quali – recependo molte delle raccomandazioni contenute nel report finale presentato dalla *National Security Commission on AI* a marzo 2021[15] – dettano norme in materia di formazione, aggiornamento e assunzione di personale provvisto di *expertise* in materia di IA[16]. Analoghe finalità sono perseguite, con un più ampio ambito di applicazione, dall'*Artificial Intelligence Training Act*, presentato a luglio 2021. Risale inoltre a maggio 2021 anche l'introduzione alla Camera dell'*Algorithmic Justice and Online Platform Transparency Act of 2021* che, oltre a tentare di arginare gli effetti potenzialmente discriminatori della profilazione online, obbliga i gestori delle piattaforme ad illustrare agli utenti in modo comprensibile i procedimenti algoritmici da essi impiegati e a potenziarne la tracciabilità, anche al fine di garantire un più efficace controllo *ex post*. Lo scorso giugno è stato inoltre nuovamente presentato un progetto di legge che ambisce, fra le altre cose, ad istituire un organismo *ad hoc* all'interno della *National Highway Traffic Safety Administration* (di seguito NHTSA) provvisto di competenze normative in materia di regolazione dei veicoli a guida autonoma[17]. Rispetto a tale settore, si ricorda inoltre la coeva pubblicazione da parte del *Department of Transportation* della *Spring Regulatory Agenda*, con la quale il Dipartimento ha raccomandato l'introduzione di standard di sicurezza rigorosi in materia di veicoli a guida autonoma, il cui rispetto dovrebbe essere assicurato tramite controlli *ex ante*, quale ad esempio l'autorizzazione al commercio dei medesimi, e sistemi di monitoraggio *ex post*, a partire dall'istituzione di un registro pubblico nazionale per documentare gli incidenti in cui essi siano coinvolti. L'NHTSA ha a questo proposito adottato un *general order* con il quale ha imposto ai produttori di veicoli provvisti di determinati *automated driving systems* di riferire eventuali incidenti all'agenzia, al fine di consentire a quest'ultima di esercitare un controllo tempestivo[18]. Similmente, l'e.o. 13981 di gennaio 2021 – uno degli ultimi della presidenza Trump – ha introdotto la policy che vieta di

[15] La *National Security Commission on AI* è stata istituita con il *National Defense Authorization Act for Fiscal Year 2019* di agosto 2018. Nonostante alcune incertezze iniziali, la giurisprudenza ha qualificato la *Commission* come una *temporary organization*, anziché un'*agency* ai sensi dell'*Administrative Procedure Act*; ciononostante, essa è tenuta ad osservare le norme in materia di diritto di accesso e trasparenza stabilite dal FOIA e dal *Federal Advisory Committee Act* (cfr. *Elec. Privacy Info. Ctr. v. Nat'l Sec. Comm'n on Artificial Intelligence* (466 F. Supp. 3d 100 (D. D.C., 2020)).

[16] Si tratta dell'*Artificial Intelligence Capabilities and Transparency Act of 2021* e dell'*Artificial Intelligence for the Military Act of* 2021. Tali proposte di legge non sono peraltro nuove, se solo si considera che già il 16 giugno 2020 era stato presentato al Senato l'*Artificial Intelligence for the Armed Forces Act of 2020*.

[17] Si tratta del c.d. *SELF Drive Act* (ossia il *Safely Ensuring Lives Future Deployment and Research Act*).

[18] In ragione dei termini in cui sono definiti gli ADS, l'ambito di applicazione del *general order*, datato 29 giugno 2021, è tuttavia piuttosto limitato. Nondimeno, l'agenzia ha anche sottoposto ad *advance notice of proposed rulemaking* una *Framework for Automated Driving System Safety* (49 CFR 571, 2021), dimostrandosi intenzionata ad adottare nuovi e più rigorosi standard di sicurezza in questo settore.

impiegare risorse pubbliche per l'acquisto o lo sviluppo di *unmanned aircraft systems* che presentino *unacceptable risks*, che siano prodotti da *foreign adversaries* o che comunque contengano componenti essenziali provenienti da questi ultimi[19]. Di particolare rilievo, specie per il raffronto con la normativa europea, è infine l'introduzione al Senato del *Data Protection Act of 2021*[20]. Quest'ultimo, oltre a prevedere l'istituzione di un'agenzia federale per la protezione dei dati personali dotata di poteri regolatori, di vigilanza e sanzionatori (§§10-13), contiene una disposizione *ad hoc* per i sistemi automatici di trattamento dei dati e di decisione (§2(3)), i quali vengono qualificati *ex lege* in termini di pratica ad alto rischio (§2(11)), circostanza che impone un'adeguata valutazione di impatto ed un *risk assessment* (§2(12)-(13)).

Per quanto indicative della direzione in cui va evolvendo il dibattito parlamentare, non pare superfluo ricordare che quelle sin qui brevemente richiamate sono quasi esclusivamente proposte di legge, che solo in un numero limitato di casi si sono tradotte in norme di diritto positivo vigenti.

Quanto invece agli interventi settoriali posti in essere dalle singole agenzie, questi ultimi vanno inquadrati entro l'approccio *hands-off* alla regolazione dell'intelligenza artificiale delineato dal memorandum "*Guidance for Regulation of Artificial Intelligence Applications*" di novembre 2020. Con tale atto il Direttore dell'OMB ha infatti esortato le agenzie federali ad evitare azioni che «needlessly hamper AI innovation and growth» e ad astenersi dall'adottare un «precautionary approach that holds AI systems to an impossibly high standard … that could undermine America's position as the global leader in AI innovation». Esso, ancora, ha stabilito che «where a uniform national standard for a specific aspect of AI is not essential … agencies should consider forgoing regulatory action»[21]. Tutto ciò, peraltro, senza disconoscere che un impiego incontrollato dell'IA possa comportare dei rischi, ma precisando che «it is not necessary to mitigate every foreseeable risk; in fact, a foundational principle of regulatory policy is that all activities involve tradeoffs»[22]. Da tali premesse discende, secondo il Direttore dell'OMB, la necessità che le agenzie valutino attentamente se

[19] Si tratta dell'e.o. intitolato *Protecting the United States from Certain Unmanned Aircraft Systems*, del quale si veda in particolare §1. Tra i *foreign adversaries* sono inclusi, per espressa previsione del §6: Corea del Nord, Iran, Cina, Russia. Da ciò emerge enfaticamente la connessione della regolazione dell'IA con le dinamiche geopolitiche e la centralità dell'obiettivo di mantenere la *leadership* statunitense cui si è fatto riferimento nel paragrafo introduttivo.

[20] La proposta di legge è stata presentata il 17 giugno 2021.

[21] OMB, *Guidance for Regulation of Artificial Intelligence Applications*, 17 novembre 2020, 2. In termini analoghi, peraltro, già una *request for information* condotta ai tempi dell'Amministrazione Obama dal *National Science and Technology Council Committee on Technology* mostrava come «the general consensus … was that broad regulation of AI research or practice would be inadvisable at this time» e che, al contrario, «the goals and structure of existing regulations were sufficient» (si veda a questo proposito il già citato report *Preparing for the Future of Artificial Intelligence*, p. 17).

[22] Id., 3-4.

intervenire e prediligano *non-regulatory approaches*, quali ad esempio l'adozione di *policy guidance* settoriali, programmi pilota, sperimentazioni, *standards* e *frameworks* volontari[23]. In coerenza con tale quadro, la regolazione dell'IA finisce di fatto per essere ampiamente affidata alla *self-regulation*; quest'ultima tuttavia, come osservato altrove, ha già mostrato alcuni limiti e posto rilevanti criticità[24]. È alla luce di tale contesto che le agenzie federali hanno avviato alcuni procedimenti di *rulemaking*. Questi ultimi, tuttavia, si trovano ancora, nella maggior parte dei casi, in una fase iniziale del processo di regolazione[25].

Occorre infine volgere un rapido sguardo alla dimensione statale della regolazione dell'IA, specie se si considera che i legislatori statali si sono dimostrati significativamente più attivi e rapidi del Congresso federale. Oltre all'introduzione di innumerevoli proposte di legge aventi i contenuti più disparati[26], si registra in un numero consistente di Stati l'istituzione – con legge – di nuove autorità amministrative competenti in materia di IA e dotate, in prevalenza, di funzioni consultive[27]. Ciò rivela come la scelta delle istituzioni politiche – al tempo stesso inevitabile e condivisibile – di affidarsi ad organismi tecnici, già emersa a livello federale, trovi conferma anche a livello statale.

2.2. Brevi cenni sulla regolazione dei sistemi di riconoscimento biometrico

Tra le applicazioni più controverse dell'IA si annoverano, come noto, i sistemi di riconoscimento biometrici. Questi ultimi, come messo in luce da un report pubblicato dal GAO a giugno 2021[28], sono già impiegati pressoché

[23] Id., 7 ss.
[24] Sul punto si rimanda a E. Chiti, B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, cit., in particolare 43 ss., e L. Parona, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici*, soft law *e* self-regulation, cit., in particolare 85 ss.
[25] A titolo esemplificativo si ricordano qui le *requests for information and comment* e le *advanced notices of proposed rulemaking* prodromiche all'adozione di *formal rules* indette dal *Nuclear Research Council* in relazione all'impiego di sistemi intelligenti nel settore nucleare (21 aprile 2021), dal *Department of Treasury* e dal *Bureau of Financial Consumer Protection* in merito all'impiego di algoritmi di *machine learning* da parte delle istituzioni finanziarie (4 maggio 2021), dalla *Food and Drugs Administration* (18 gennaio 2021), e dalla NHTSA in materia di veicoli a guida autonoma (3 dicembre 2020).
[26] Alcune di queste hanno recentemente completato l'*iter legis*, come nel caso del Colorado che ha introdotto il divieto di impiegare determinati algoritmi predittivi nel settore assicurativo (CO S.B. 169, 2021). In argomento si veda anche, in questo fascicolo, E. Stradella, *Le fonti nel diritto comparato*.
[27] Cfr. Alabama (AL S.B. 78, 2021, e AL SJR 71, 2019), Hawaii (HI SR 142, 2019) Illinois (IL H.B. 645, 2021), New York (NY S.B. 3971, 2019), Utah (UT S.B. 96, 2020), Vermont (VT H.B. 16, 2019, e VT H.B. 378, 2018), Washington (WA S.B. 6544, 2017). A questi si aggiungono California e New Jersey, nei quali commissioni *ad hoc* sono state istituite, rispettivamente nel 2020 e nel 2018, con atto dei Governatori.
[28] GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, giugno 2021, che analizza i sistemi di riconoscimento biometrici impiegati da venti agenzie federali e le relative criticità.

da tutte le agenzie federali titolari di funzioni di *law enforcement*, le quali si avvalgono di una pluralità di tecnologie che differiscono fra loro sotto numerosi punti di vista. Un aspetto accomuna tuttavia la maggior parte di tali sistemi – in particolare quelli di riconoscimento facciale – ossia l'impiego di un database privato (*Clearview AI*) che, consentendo il raffronto con un bacino di oltre tre miliardi di immagini, supera per dimensioni tutti i database pubblici delle amministrazioni – federali e statali – americane[29]. Poiché l'attendibilità di tali sistemi di riconoscimento a fini di verificazione (*one-to-one matching*) e identificazione (*one-to-many matching*) non è – quantomeno allo stato attuale – tale da escludere il rischio di incorrere in falsi positivi e falsi negativi e di generare output discriminatori, è stata introdotta nel 2020, e poi ripresentata a giugno 2021, una proposta di legge volta a vietare in termini generalizzati l'impiego di questi ultimi da parte delle agenzie federali[30]. Più precisamente, ai sensi di tale proposta nessuna agenzia potrebbe – più – impiegare sistemi di riconoscimento facciale a meno che questi ultimi non vengano specificamente e singolarmente approvati dal Congresso con un atto legislativo, il quale, fra le altre cose, dovrebbe prevedere puntuali requisiti e meccanismi di controllo. Tale disegno di legge prevede anche un *private right of action* per i cittadini nei cui confronti dovessero essere impiegati tali sistemi di riconoscimento in spregio del divieto legislativo[31]. Il dibattito parlamentare è tuttavia in corso e, per acquisire input dalla società civile, il *National AI Initiative Office* ha avviato ad agosto 2021 una consultazione pubblica sugli impieghi attuali e potenziali di tali sistemi di riconoscimento[32].

Come noto, invece, alcune autorità locali sono state più risolute di quelle federali nel regolare, vietandone l'utilizzo, i sistemi di riconoscimento facciale[33]. Una soluzione intermedia è stata introdotta a marzo 2020 nello Stato di Washington, il cui Congresso ha approvato una legge che impone alle amministrazioni pubbliche di rendere noto l'utilizzo di sistemi di riconoscimento facciale ed il relativo grado di accuratezza rispetto all'etnia,

[29] Id., p. 16.
[30] Si tratta del già citato (v. *supra* par. 2.1) *Facial Recognition and Biometric Technology Moratorium Act* introdotto il 25 giugno 2020 al Senato e ripresentato il 15 giugno 2021. Di tenore analogo è anche il *Commercial Facial Recognition Privacy Act of 2019* (introdotto al Senato il 14 marzo 2019 e mai messo in votazione) il quale prevede l'introduzione di un analogo divieto anche per gli operatori privati.
[31] Tale proposta mira ad incidere anche sull'impiego dei sistemi di riconoscimento facciale da parte delle autorità statali, prevedendo che queste ultime possano ricevere risorse federali solamente laddove lo Stato in questione approvi una legge o una *policy* sostanzialmente analoga a quella introdotta a livello federale.
[32] Tra le applicazioni potenziali, la consultazione fa riferimento all'impiego dei sistemi di riconoscimento biometrici per finalità predittive, quale ad esempio la c.d. *intent inference*, volta a dedurre dai movimenti corporei e dalle espressioni del viso le intenzioni di un determinato soggetto, al fine di anticiparne le azioni.
[33] A partire da maggio 2019 una decina di grandi città statunitensi ha introdotto tali divieti, tra di esse si ricordano qui San Francisco, Portland, Oakland, e Boston.

al sesso e all'età dei cittadini[34]. La legge impone inoltre un "*meaningful human review*" quando l'utilizzo di tali tecnologie sia strumentale all'assunzione di *major decisions* e pone limitazioni significative all'impiego delle medesime nel settore dell'ordine pubblico e delle attività di polizia, fatta eccezione per le situazioni emergenza.

Un significativo esempio proviene infine dallo Stato dell'Illinois, che già nel 2008 aveva approvato il *Biometric Information Privacy Act*, il quale vieta la raccolta e l'utilizzo di dati biometrici da parte di soggetti privati senza il consenso degli interessati, anche quando tali dati (incluse le immagini) siano liberamente accessibili su pagine e profili pubblici di un *social network*[35].

3. L'approccio europeo

Se il quadro regolatorio statunitense appare ancora indefinito e frammentato, oltre che abitato principalmente da atti di *soft law*, la Commissione europea ha emanato nell'aprile scorso una proposta di regolamento che mira a disciplinare l'intelligenza artificiale (*Artificial Intelligence Act*, d'ora in poi AIA) secondo un disegno unitario, organico e completo, applicabile su tutto il territorio dell'Unione[36]. Si tratta di una normativa che sposa un approccio proporzionato al rischio e che scommette sulla propria capacità di bilanciare adeguatamente opportunità e istanze di crescita legate alla ricerca e allo sviluppo dell'IA con i rischi che alcune applicazioni di IA presentano per i diritti fondamentali e la privacy dei cittadini. Da tale disciplina discenderà l'assetto della materia negli Stati membri dell'Ue[37], i quali ultimi saranno anche chiamati a darvi attuazione attraverso la creazione di apposite amministrazioni, secondo i principi dell'amministrazione indiretta, e attraverso l'adozione di specifici codici di condotta[38].

[34] WA S.B. 6280, 2020.

[35] Per una recente applicazione delle norme previste da tale legge si veda il caso *Vance v. Microsoft Corp.* (W.D. Wash., 15 marzo 2021). In tale controversia una coppia di cittadini dell'Illinois che aveva pubblicato sul proprio profilo pubblico di un *social network* alcune fotografie (che ne ritraevano il volto) ha convenuto in giudizio Microsoft per aver impiegato queste ultime, senza il loro consenso, al fine di alimentare il database di un *software* di riconoscimento facciale.

[36] La proposta giunge al termine di un percorso inaugurato dal Libro Bianco sull'IA del 19 febbraio 2020, cui sono seguite le consultazioni che si sono concluse nel maggio 2020. Essa inoltre beneficia delle linee guida elaborate dallo *High Level Expert Group on AI* (*Trustworthy AI*, 8 aprile 2019) e della valutazione di impatto da parte del *Regulatory Scrutiny Board* della Commissione.

[37] La scelta del Regolamento in luogo della Direttiva comporta la creazione di vincoli uniformi e direttamente applicabili su tutto il territorio dell'Unione europea e sottrae agli Stati quei margini di manovra sostanziali che lo strumento della direttiva avrebbe lasciato loro, ad eccezione di alcuni specifici istituti quali le sandboxes e i codici di condotta, e alcuni profili organizzativi e sanzionatori.

[38] Per un commento alla proposta sia consentito rinviare a C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di*

La proposta comporta anche la creazione di un Board europeo per l'IA e l'attribuzione di alcune competenze fondamentali alla Commissione. In particolare, al fine di garantire l'aggiornamento continuo e la necessaria messa a punto del regolamento in corrispondenza dei rapidi e incessanti sviluppi tecnologici che connotano la materia, spetterà alla Commissione esercitare i poteri normativi (delegati) di cui all'art. 290 TFUE per modificare gli allegati alla proposta di regolamento in cui sono inseriti rilevanti elementi in vista della individuazione delle categorie di rischio e le procedure di verifica della conformità.

Benché si possa prevedere che nel procedimento per giungere alla approvazione da parte di Parlamento e Consiglio la disciplina subirà delle modifiche, l'impianto complessivo e l'approccio europeo alla regolazione dell'IA sono ben delineati. È evidente, in particolare, che si tratta di un approccio tutt'altro che *hands-off*, anche se – come vedremo – la sua capacità di conciliare i vantaggi dell'IA con la protezione effettiva dei diritti e della privacy degli utilizzatori dipenderà in larga parte dal funzionamento concreto dei meccanismi di controllo in esso previsti.

3.1. La proposta di AIA in pochi punti

Un primo elemento che deve essere sottolineato della proposta europea è il suo perimetro di applicazione. Essa mira a raggiungere non solo programmatori, produttori e fornitori localizzati in Paesi europei, ma prende a riferimento la circolazione (e messa in servizio) del prodotto sul mercato europeo, qualunque sia il luogo della sua produzione, fino ad inseguire ogni sistema di IA i cui output siano utilizzati nel territorio dell'Ue. Si tratta di quello che Anu Bradford ha definito *The Brussels Effect*, ossia «the EU's unilateral power to regulate global markets»[39]. Ciò significa che i sistemi di IA sviluppati negli Stati Uniti o in Cina potranno essere utilizzati e commercializzati sul territorio dell'Unione solo se saranno conformi alla disciplina adottata a Bruxelles.

Il secondo elemento su cui occorre soffermare l'attenzione è l'approccio regolatorio basato sul rischio: la disciplina stabilisce un diverso trattamento giuridico dei sistemi di IA a seconda dei rischi potenziali per i diritti fondamentali, la sicurezza e la privacy dei cittadini. In particolare, si distinguono quattro categorie di IA: anzitutto sono individuati i sistemi vietati (salvo eccezioni) in ragione dei rischi inaccettabili che possono creare (art. 5); poi è stabilita la categoria dei sistemi ad alto rischio, per la quale si prevede una procedura di verifica di conformità a determinati requisiti di "affidabilità" (art. 6); e poi vi sono i sistemi a basso o minimo rischio, per i quali è prevista la libera circolazione nel mercato, salvi alcuni obblighi di informazione che possono essere stabiliti a garanzia dell'utilizzatore (art. 52).

intelligenza artificiale, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2021, 415.
[39] A. Bradford, *The Brussels Effect. How the European Union rules the world*, Oxford, 2020.

DPCE online
ISSN: 2037-6677

Per comprendere i tratti distintivi delle diverse categorie di IA è fondamentale, oltre al testo degli articoli sopra ricordati, quanto contenuto negli allegati alla proposta di regolamento, soprattutto per l'identificazione dei sistemi ad alto rischio. Tuttavia, anche così, le categorie di rischio si prestano a qualche incertezza interpretativa. Ad esempio, la proposta considera vietate, tra le altre, le applicazioni di IA usate da autorità pubbliche per stabilire l'affidabilità delle persone (*social scoring*) solo quando il punteggio sociale comporta un trattamento pregiudizievole o sfavorevole «in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti», oppure quando il trattamento sfavorevole sia «ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità» (art. 5 par. 1 lett. c)).

Analoghi spazi di manovra sono stabiliti nelle disposizioni che riguardano l'uso di sistemi di identificazione biometrica, il cui impiego può avvenire tenendo conto della natura della situazione che dà luogo al possibile uso» e le «conseguenze dell'uso del sistema per i diritti e le libertà», in particolare «la gravità, la probabilità e l'entità di tali conseguenze» (art. 5 par. 2 lett. a) e b)).

L'art. 6 e l'allegato 3 individuano i sistemi ad alto rischio e i settori di riferimento: si tratta, in particolare, dei sistemi di identificazione biometrica ammessi, dei sistemi utilizzati come componenti di sicurezza per la gestione delle infrastrutture critiche, dei sistemi utilizzati per l'accesso o la valutazione nell'istruzione e nella formazione professionale, per l'assunzione, selezione e promozione nell'occupazione e gestione dei lavoratori, nell'accesso al credito e ai servizi pubblici, nella sanità, nella polizia, nell'amministrazione della giustizia, nell'ambito dei processi democratici e nell'immigrazione. È evidente quanto la sfera delle funzioni e dei servizi pubblici sia destinata ad essere toccata dalle nuove regole. Ai sistemi ad alto rischio è dedicata la gran parte della disciplina, la quale stabilisce che la loro commercializzazione e messa in servizio sia condizionata da una verifica di conformità dell'IA ai requisiti stabiliti nel capo II del regolamento. In particolare, il fornitore di un sistema con questa componente di rischio deve dotarsi di un sistema di gestione del rischio, deve utilizzare dati accurati (e seguire un sistema di *data governance* che scongiuri errori e *bias*), deve assicurare un appropriato livello di trasparenza sul funzionamento della macchina (l'art. 13, consapevole dell'opacità dei sistemi *machine learning*, parla di funzionamento «sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente») e deve, infine, garantire la possibilità della sorveglianza umana (*human in the loop*): l'interazione uomo-macchina, infatti, è fondamentale per prevenire o ridurre al minimo «i rischi per la salute, la sicurezza o i diritti fondamentali», sia che sia integrata nel sistema dal fornitore sia che venga attuata dall'utente.

Tale garanzia deve non solo assicurare l'individuazione di

malfunzionamenti del sistema e la loro correzione, ma anche rendere consapevoli gli utilizzatori «della possibile tendenza a fare automaticamente affidamento (o a fare eccessivo affidamento) sull'output prodotto da un sistema ad alto rischio ("distorsione dell'automazione"[40]), in particolare per i sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche».

Il terzo elemento capace di svelare la portata della regolazione europea riguarda i sistemi di verifica del rispetto da parte delle applicazioni di IA dei requisiti appena ricordati. Poiché è da tali verifiche che dipende l'effettività delle garanzie contenute nel regolamento a protezione dei diritti, occorre assicurare che tali meccanismi di controllo funzionino efficacemente. Qui sta forse un fattore di possibile criticità della disciplina, ossia la previsione che – con l'eccezione dei sistemi biometrici – sarà lo stesso provider ad operare la verifica di conformità e ad apporre il marchio necessario per la commercializzazione o la messa in servizio del sistema, al pari di quanto accade, ad esempio, per il controllo di sicurezza dei giocattoli o di altri prodotti ammessi a circolare nell'Ue.

Evidentemente la Commissione considera sufficiente tale regime di auto-controllo, accompagnato da sanzioni severe per il caso di violazioni, sia rispetto ad una procedura di autorizzazione amministrativa (quale quella prevista, per esempio, in materia di medicinali o di OGM), la quale presenterebbe lo svantaggio di rallentare l'ingresso dei sistemi di IA nel mercato, sia rispetto ad una verifica di conformità assegnata a soggetti verificatori terzi rispetto al provider. Può essere che tale scelta dipenda dalla necessità di assicurare un'immissione rapida nel mercato anche in ragione degli sviluppi tecnologici repentini che connotano i prodotti tecnologici, o dalla fiducia nella funzione deterrente del regime sanzionatorio, ma va da sé che la protezione dei diritti fondamentali dipenderà dalla efficacia di questi controlli e del monitoraggio post-market che il regolamento affida a utilizzatori, fornitori e autorità di sorveglianza nazionali. Con l'avvertenza, tuttavia, che proprio la flessibilità regolatoria resa possibile dagli allegati alla proposta potrà, a fronte di risultati poco soddisfacenti dell'attuale sistema, consentire un passaggio agevole alla procedura che affida a soggetti terzi ed imparziali (verificatori) i controlli di sicurezza dei sistemi di IA[41].

[40] Secondo quello che in A. Garapon, J. Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique*, Parigi, 2018 gli autori chiamano effetto *moutonnier* riferito alla giustizia predittiva che porterebbe il giudice ad affidarsi eccessivamente alla macchina. Il pericolo è segnalato anche da A. Simoncini, *L'algoritmo incostituzionale: l'intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 69. Sul rapporto tra IA e giustizia cfr. C. Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE online*, 3, 2020, 3369; F. Donati, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, 1, 2020, 415; S. Arduini, *La "scatola nera" della decisione giudiziaria: tra giudizio umano e giudizio algoritmico*, in *BioLaw Journal – Rivista di BioDiritto*, 2, 2021, 453.

[41] Tale passaggio diventa agevole perché l'art. 43 della proposta di AIA, laddove stabilisce la procedura per la valutazione di conformità, rinvia all'allegato III per

DPCE online
ISSN: 2037-6677

3.2. I sistemi di identificazione biometrica nella proposta di regolamento Ue

Quanto osservato sui sistemi di identificazione biometrica nel contesto statunitense ci consegna un primo dato rilevante, che consiste nella mancanza, ad oggi, di una disciplina federale generale, e nella presenza di fonti normative che li disciplinano sia a livello dei singoli Stati, sia a livello di città, fissando un regime di tendenziale divieto in caso di utilizzo per finalità di polizia. L'assenza di un quadro generale di riferimento di provenienza del Congresso porta con sé, dunque, la frammentarietà delle scelte regolatorie all'interno degli Stati Uniti, con ciò che ne consegue in termini di disparità di trattamento e di incertezza. Inoltre, il ritardo del Congresso nel disciplinare la materia fa si che le agenzie federali stiano ampiamente utilizzando tali sistemi, in particolare quello di riconoscimento facciale, al di fuori di una cornice di regole che assicuri la tutela della privacy e protegga il cittadino dai ben noti rischi discriminatori legati a tali sistemi.

La situazione europea non è molto diversa da quella nordamericana, mancando ancora, ad oggi, una disciplina generale, sicché in attesa dell'approvazione del regolamento sull'IA l'impiego dei sistemi biometrici non trova limiti diversi da quelli posti dal GDPR e negli atti di *soft law*. Tuttavia, la disciplina europea contenuta nella proposta di AIA promette di regolare uniformemente la materia su tutto il territorio dell'Unione, stabilendo un regime di divieto per il loro impiego a scopi di *law enforcement*, e in altri casi sottoponendoli alla verifica di conformità da parte di organismi terzi verificatori. Benché, infatti, l'attuale quadro di regole non elimini, come detto, ogni spazio di manovra dei legislatori statali, esso prefigura comunque un trattamento per larghi tratti necessariamente convergente nei diversi Paesi membri.

Ad oggi i sistemi biometrici sono tendenzialmente vietati se operanti *in tempo reale*, *in spazi accessibili al pubblico* e per *finalità di polizia* (*law enforcement*), e le eccezioni a tale regola sono comunque circostanziate e giustificate per: «la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi» (i); «la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico» (ii) o «il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o di un sospettato di reati individuati e punibili con una pena di almeno tre anni» (iii). Il quadro dei divieti risulta così sufficientemente definito a livello europeo, con pochi spazi interpretativi alla luce della *natura e gravità della situazione*, della *entità dei danni*, delle *conseguenze per le libertà* e dell'entità di queste ultime, e fermo restando il rispetto del *principio di proporzionalità*, «in particolare per quanto

l'individuazione dei sistemi ad alto rischio che possono utilizzare la procedura interna o che devono utilizzare quella esterna, che richiede cioè l'intervento di un organismo notificato terzo rispetto al fornitore. In tal modo, la modifica di tale allegato consente indirettamente anche di incidere sulla tipologia di procedura di controllo imposta al provider.

riguarda le limitazioni temporali, geografiche e personali». L'impiego dei sistemi biometrici in tempo reale e in spazi accessibili al pubblico è inoltre subordinato ad un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro competente, la quale verificherà le condizioni previste dal regolamento per superare un divieto altrimenti generale.

La previsione di eccezioni circostanziate alla regola del divieto e le cautele che ne concernono l'applicazione – prima fra tutte la necessaria autorizzazione preventiva – dovrebbero evitare abusi nel ricorso a tali applicazioni e rispondere adeguatamente alla forte preoccupazione di errori e *bias* legata al funzionamento di tali sistemi quando è in gioco la libertà personale: un rapporto dello US *National Institute of standards and technology* non lascia dubbi, infatti, sull'alta percentuale di falsi positivi prodotta dal suo funzionamento, soprattutto tra la popolazione di colore e asiatica[42].

4. Conclusioni

Al termine di questa breve disamina, pare di poter dire che l'avvicendamento alla presidenza degli Stati Uniti non sia stato accompagnato da discontinuità significative quanto al settore qui preso in considerazione. Non è infatti mutato l'approccio *hands-off* alla regolazione, né l'attenzione per la tutela dei diritti dei cittadini rispetto ai possibili rischi posti dall'impiego dell'intelligenza artificiale pare aver ridefinito le priorità delle istituzioni politiche, tra le quali il mantenimento della *leadership* statunitense si conferma al primo posto sebbene, come visto, siano ravvisabili i segnali di una maggiore presa di coscienza di tali aspetti.

Dal canto suo, l'Unione europea è impegnata a delineare un quadro normativo sempre più completo e articolato in grado di affrontare le sfide poste dalla tecnologia digitale: oltre ai numerosi atti normativi già approvati (*General Data Protection regulation* (GDPR), il *Digital Services Act* il *Digital Markets Act* e la strategia in tema di *Cybersecurity*), la proposta di regolamento in materia di IA, qui esaminata, e la risoluzione del Parlamento europeo dell'ottobre 2020 concernente raccomandazioni rivolte alla Commissione su un regime di responsabilità civile per l'IA mirano a disegnare regole certe,

[42] Il tema è dibattuto: tra i molti v. K. Crawford, *Halt the use of facial-recognition technology until it is regulated*, in *Nature*, 572, 2019, 565; R. Richardson, *Facial Recognition in the public sector: the policy landscape*, in *Jstor*, 2021. La previsione a livello europeo di precisi limiti alle deroghe al divieto di utilizzo del riconoscimento facciale dovrebbe impedire agli Stati di prevedere autorizzazioni generalizzate "a maglie larghe", come pure la proposta di regolamento prevede. Prevede infatti il paragrafo 4 che «uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto entro i limiti e alle condizioni di cui al paragrafo 1 lettera d) e ai paragrafi 2 e 3». Tuttavia, la stessa disposizione, al fine di controllare tale potere dello Stato, impone oneri specifici di motivazione ed una regolamentazione dettagliata e precisa.

DPCE online
ISSN: 2037-6677

comuni ed eticamente sostenibili sul terreno più avanzato e delicato dell'innovazione tecnologica. Tale sforzo, che regala all'Ue il primato di regolatore mondiale del settore, costituisce, soprattutto se confrontato con l'esperienza degli Stati Uniti, un pregevole tentativo di trovare un equilibrio soddisfacente tra istanze di sviluppo e tutela dei diritti fondamentali e dei valori fondanti dell'Unione europea.

Rispetto alla proposta europea, invece, gli Stati Uniti non sembrano per ora seguire un approccio organico all'IA, se non nei termini estremamente generici degli e.o. adottati dall'ex-Presidente Trump. Negli USA sta prevalendo, infatti, un approccio parcellizzato – per settori e per questioni – alla regolazione dell'IA[43]. Inoltre, lo *hands-off approach* statunitense pare escludere, fatta eccezione per alcune limitate ipotesi, tanto strumenti di controllo *ex ante*, quali i sistemi di autorizzazione, accreditamento e certificazione, quanto meccanismi di controllo *ex post*, i quali invece trovano spazio nell'impianto normativo europeo.

Accanto a tali differenze, una convergenza pare tuttavia ravvisarsi nell'adozione, da entrambi i lati dell'Atlantico, di un *risk-based approach*, anche se – guardando alle proposte di legge presentate al Congresso e al memorandum del Direttore dell'OMB – la soglia di rischio tollerata negli Stati Uniti appare sensibilmente più elevata rispetto a quella che la proposta di AIA tenta di individuare.

Barbara Marchetti
Dip.to di Giurisprudenza
Università degli Studi di Trento
barbara.marchetti@unitn.it

Leonardo Parona
Scuola Superiore Meridionale
Università degli Studi di Napoli Federico II
leonardo.parona@unina.it

[43] Concorda sul punto anche E. Stradella, *Le fonti nel diritto comparato*, in questo fascicolo, che parla a questo proposito di un approccio alla regolazione "a geometria variabile".