RIVISTA QUADERNI AISDUE

FASCICOLO SPECIALE 2/2024

L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive

a cura di
Federico Ferri

Editoriale Scientifica

RIVISTA QUADERNI AISDUE

ES

ISSN 2975-2698

euro 50,00

Direttore Responsabile
Antonio Tizzano

Comitato scientifico
Adelina Adinolfi, Giandonato Caggiano, Patrizia De Pasquale,
Alessia Di Pascale, Pietro Manzini, Roberto Mastroianni, Paolo Mengozzi,
Paola Mori, Bruno Nascimbene, Francesco Rossi Dal Pozzo,
Lorenzo Schiano di Pepe, Fabio Spitaleri, Antonio Tizzano,
Ennio Triggiani, Jacques Ziller

Comitato di redazione Quaderni AISDUE
Andrea Circolo e Benedetta Minucci (coordinatori),
Mario Barbano, Samuele Barbieri, Camilla Burelli, Federico Ceci, Angela
Correra, Alessandra Favi, Federico Ferri, Miriana Lanotte,
Irene Marchioro, Gabriella Perotto, Martina Previatello,
Alessandro Rosanò, Gabriele Rugani

Coordinatori BlogDUE
Patrizia De Pasquale e Fabio Spitaleri

Comitato di redazione BlogDUE
Irene Agnolucci, Mario Barbano, Samuele Barbieri, Nicola Bergamaschi,
Camilla Burelli, Federico Ceci, Andrea Circolo, Erika Colombo,
Angela Correra, Alessandra Favi, Marta Ferrari, Federico Ferri,
Marco Gerbaudo, Anna Kompatscher, Clara Labus, Miriana Lanotte,
Irene Marchioro, Martina Minardi, Benedetta Minucci, Maria Patrin,
Gabriella Perotto, Martina Previatello, Alessandro Rosanò,
Gabriele Rugani, Enrico Tinti, Alessia Voinich

RIVISTA QUADERNI AISDUE

FASCICOLO SPECIALE N. 2/2024

"L'UNIONE EUROPEA E LA NUOVA DISCIPLINA
SULL'INTELLIGENZA ARTIFICIALE: QUESTIONI E PROSPETTIVE"

a cura di
Federico Ferri

Editoriale Scientifica
Napoli

L'invio di un manoscritto presuppone l'adesione al codice etico della Rivista e l'uniformità dello stesso ai criteri redazionali (consultabili online all'indirizzo www.aisdue.eu).

I contributi sono sottoposti a previo referaggio cieco anonimo secondo i principi descritti nel codice etico e nella procedura di revisione.
Tutti i lavori devono essere inviati in formato word all'indirizzo info@aisdue.eu.

Proprietà letteraria riservata

© Copyright 2024 Editoriale Scientifica srl
via San Biagio dei Librai, 39
80138 Napoli
ISSN 2975-2698

INDICE

Prefazione di Cristina Schepisi 7
Introduzione di Federico Ferri 15

Articoli

ZACCARONI G., *Intelligenza artificiale e principio democratico: riflessioni a margine dell'emersione di un quadro normativo europeo* 19

CIRONE E., *L'*AI Act *e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali* 51

INGLESE M., *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno* 71

VOLPATO A., *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale* 91

FERRI F., *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea* 107

VILLANI S., *Il sistema di vigilanza sull'applicazione dell'*AI Act: *ognun per sé?* 125

RUGANI G., *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'*AI Act, *con particolare riferimento alle* regulatory sandboxes 143

GRIECO C., *Il diritto d'autore nell'*AI Act: Error 404 – Page Not Found*?* 157

LATTANZI S., *Prime riflessioni sull'applicazione del nuovo regolamento sull'intelligenza artificiale al settore sanitario* 181

CORRERA A., *Il ruolo dell'Intelligenza artificiale nel paradigma europeo dell'*E-justice*. Prime riflessioni alla luce dell'*AI Act 209

BURELLI C., *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?* 237

Prefazione

di *Cristina Schepisi*

1. I sistemi e le applicazioni che usano l'intelligenza artificiale (IA) consentono innegabili benefici, sia economici che sociali ma dall'altro possono, come noto, comportare rischi, anche molto elevati, di lesione dei diritti fondamentali, della *rule of law* e dei principi democratici. L'opacità, la complessità, la dipendenza dai dati, il comportamento autonomo sono tutte caratteristiche dei sistemi di IA che possono incidere negativamente su una serie di diritti protetti dalla Carta europea.

A fronte di tali questioni, e dopo un *iter* procedurale durato tre anni dall'iniziale proposta formulata dalla Commissione (COM (2021)206 def., 21 aprile 2021), il Regolamento UE sull'intelligenza artificiale è stato finalmente approvato il 21 maggio 2024 (per entrare in vigore dopo due anni dalla pubblicazione nella Gazzetta Ufficiale dell'Unione europea).

Nel suo *Libro Bianco sull'intelligenza artificiale* (19.2.2020 COM (2020) 65 final), la Commissione aveva ben messo in luce l'intento di mantenere il delicato equilibrio tra l'esigenza di «preservare la leadership tecnologica dell'UE», incoraggiando le imprese a sviluppare le soluzioni basate sull'IA», e la necessità di assicurare «che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione».

Tra le varie soluzioni che erano state studiate, la scelta di procedere con una regolamentazione trasversale ha prevalso su quella di disciplinare verticalmente i diversi settori (o solo alcuni di essi, es. lavoro, sanità, istruzione, giustizia, consumatori) nei quali i sistemi di intelligenza artificiale possono generare maggiore preoccupazione, o di intervenire direttamente e singolarmente sui diversi sistemi (prodotti, *machine learning, deep fake*, ecc.), approccio quest'ultimo che sarebbe risultato assai limitativo viste le molteplici applicazioni che un sistema di IA può avere nei vari settori e il diverso impatto che può produrre.

A tal fine, e come noto, la strada perseguita dall'Unione europea è stata quella di procedere attraverso l'adozione di un atto a portata generale (un regolamento) sulla base giuridica dell'art. 114 TFUE, e con l'obiettivo di introdurre, in capo a coloro i quali producono, mettono in servizio o usano sistemi di intelligenza artificiale, divieti, obblighi ed adempimenti procedu-

rali, calibrati sul diverso livello di rischio, valutato *ex ante* (e anche sulla base dell'utilizzo che della singola applicazione viene fatta nell'ambito dei diversi settori e in particolare di quelli più sensibili), che tali sistemi sono suscettibili di produrre per i diritti fondamentali, prescindendo dunque dalle dimensioni del fornitore e/o della piattaforma digitale.

Se l'impianto generale del Regolamento è rimasto quello inizialmente immaginato dalla Commissione (dall'identificazione dei diversi livelli di rischio dei sistemi di IA, ai conseguenti obblighi e adempimenti procedurali in capo a produttori, prestatori e utilizzatori di tali sistemi, ai divieti in caso di rischio inaccettabile, al sistema di *governance* e controllo), il Consiglio e il Parlamento europeo hanno tuttavia apportato numerosi correttivi, frutto delle preoccupazioni, del primo, di assicurare la sostenibilità dei nuovi oneri e obblighi da parte delle imprese; ma, soprattutto del secondo, di elevare la protezione dei diritti fondamentali e il rispetto dei valori dell'Unione.

Il risultato è stato, da un lato, l'inserimento di alcune deroghe che hanno "ammorbidito" in taluni casi la rigidità di alcuni adempimenti procedurali; dall'altro l'effetto è stato un'estensione dei divieti ed una maggiore accuratezza nella qualificazione dei sistemi di IA ad alto rischio con conseguente ampliamento dei casi in cui il Regolamento richiede il rispetto di obblighi ed oneri da parte dei produttori, prestatori ed utilizzatori di tali sistemi.

Da menzionare, ad esempio, tra gli altri, l'estensione del divieto dell'uso di sistemi di punteggio sociale anche da parte dei soggetti privati e non solo delle pubbliche autorità (art. 5, par. 1, lett. c); e del divieto dei sistemi che usano tecniche subliminali e manipolatorie non più solo limitato a gruppi di persone in ragione dell'età o della disabilità ma anche della *specifica situazione sociale o economica* (art. 5, par. 1, lett. b). Riguardo ai sistemi di identificazione biometrica, il Regolamento restringe la portata delle deroghe inizialmente previste in caso di uso "*in real time*".

Nella sua versione finale, il Regolamento introduce inoltre alcuni nuovi divieti come ad esempio quello relativo a sistemi per effettuare valutazioni o previsioni del rischio di commissione di reati da parte di persone fisiche; a sistemi che creano o ampliano le banche dati di riconoscimento facciale o che siano mirate a rilevare le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione; o ai sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale.

2. Nel corso delle varie letture, la difficoltà ovviamente maggiore è stata quella di difendere una regolamentazione *uniforme,* senza d'altra parte imbrigliare eccessivamente l'innovazione tecnologica e l'autonomia di produttori, sviluppatori e utilizzatori di sistemi di IA, ed evitando di comprimere il livello (auspicabilmente alto) di tutela dei diritti.

Regolare in maniera uniforme i sistemi di IA a livello di Unione evita innanzitutto la frammentazione del mercato interno, ed è questa certamente la ragione principiale del ricorso alla base giuridica dell'art. 114 TFUE. La coesistenza di distinti meccanismi di regolazione, *ex ante* o *ex post*, per singoli settori o anche a livello orizzontale, causerebbe necessariamente delle restrizioni alla libera circolazione dei servizi e dei prodotti tra uno Stato e l'altro.

Va tuttavia, e d'altro canto, banalmente osservato che interventi unilaterali degli Stati membri – diretti a seconda dei casi a proteggere o a elevare la tutela dei diritti della persona, e dunque a restringere l'immissione in commercio o la distribuzione di determinati sistemi di IA - comporterebbe anche una *frammentazione della stessa tutela di tali diritti*, oltre che del mercato, all'interno dell'Unione europea.

Una gradazione diversa della tutela dei diritti a seconda degli Stati membri rischierebbe, da un lato, di diminuire la certezza di una tutela chiara, uniforme ed elevata nello spazio europeo (e nel rispetto della Carta europea) e conseguentemente la fiducia, da parte delle persone fisiche, nei confronti di determinate applicazioni e degli strumenti di protezione. D'altro lato, potrebbe minare l'obiettivo dell'Unione europea di promuovere uno *standard* elevato e uniforme dei diritti in un contesto globale, e di spingere anche Paesi terzi ad adottare regolamentazioni analoghe o comunque a indurre sviluppatori e produttori stranieri ad adeguare l'offerta di prodotti e servizi alla normativa europea anche al di fuori di tale contesto, in ragione anche di una maggiore convenienza, e per l'effetto aumentare la protezione dei diritti (c.d. *effetto Bruxelles*).

La finalità (anche) di tutela (sia *elevata* che *uniforme*) dei diritti fondamentali, perseguita dal Regolamento, non scalfisce in ogni caso la correttezza della scelta della base giuridica dell'art. 114 TFUE, peraltro arricchita dal riferimento anche all'art. 16 TFUE (che consente alle istituzioni di adottare atti a tutela dei dati personali), né si sarebbero potute percorrere altre vie. L'art. 2 TUE, ad esempio, non legittima l'adozione di atti da parte delle istituzioni, mentre l'art. 19 TFUE, oltre ad avere un profilo limitato al principio di non discriminazione, non costituirebbe un'idonea base giuridica in ragione della procedura legislativa speciale prevista nella stessa norma (in

questo senso, A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: brevi considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *La rivoluzione dell'intelligenza artificiale: profili giuridici,* Bologna, 2022).

3. Le questioni che solleva la nuova regolamentazione sono molteplici e il presente Volume ne dà esaustivamente conto.

Uno dei contributi è dedicato proprio al rapporto, appena ora menzionato, tra l'esigenza di tutelare il mercato e l'innovazione tecnologica, da un lato, e quella di garantire un elevato *standard* di tutela dei diritti, dall'altro (Marco Inglese). Nello scritto l'autore si interroga in particolare sulla capacità del legislatore europeo, anche alla luce della giurisprudenza della Corte di giustizia, di addivenire a una sintesi tra due esigenze solo apparentemente contrapposte.

Il Volume contiene inoltre alcune riflessioni sulla capacità della nuova regolamentazione sull'intelligenza artificiale di assicurare la tenuta dei principi democratici. Ci si chiede, da un lato, se il nuovo quadro giudico europeo sia idoneo a prevenire rischi e minacce ai principi democratici (Giovanni Zaccaroni) e, dall'altro, se sia in grado di introdurre e stabilire uno standard normativo globale per l'intelligenza artificiale e promuovere i valori europei oltre i confini dell'ordinamento giuridico europeo (Enza Cirone).

Diversi contributi affrontano poi alcuni temi di carattere più squisitamente istituzionale. Viene infatti esaminata la portata della "normativa armonizzata" e spese alcune riflessioni critiche sulla compatibilità della delega di poteri a soggetti privati con i principi di diritto dell'Unione europea (Annalisa Volpato). Sono poi svolte alcune considerazioni sul sistema di *governance* e soprattutto sull'(ampia) portata dei poteri normativi e sanzionatori della Commissione (Federico Ferri). Nell'ambito della *governance* sono inoltre coinvolte anche le autorità nazionali e ci si interroga quindi sul loro ruolo e sulla necessità del rispetto del principio di leale collaborazione di cui all'art. 4, par. 3, TUE (Susanna Villani). Un ulteriore profilo esaminato è quello relativo al ruolo della co-regolazione e alla (non agevole) disciplina degli "spazi di sperimentazione normativa" (Gabriele Rugani). Riguardo ai rapporti con gli ordinamenti nazionali, e in particolare alla compatibilità di misure nazionali con il Regolamento, una specifica attenzione è rivolta al nuovo "ddl intelligenza artificiale" e alle sue ricadute istituzionali e politiche (Camilla Burelli).

Il Volume è poi arricchito da contributi che analizzano l'impatto del

nuovo Regolamento in contesti e settori di particolare rilevanza. L'IA, come noto, pone delicate questioni in materia di diritto d'autore, in particolare per quanto riguarda l'utilizzo in maniera indiscriminata dei *dataset* da parte dalle aziende nelle fasi di addestramento degli algoritmi; e per ciò che concerne la creazione di opere intellettuali direttamente realizzate da sistemi di intelligenza artificiale (Cristina Grieco). Tra i vari settori a maggiore impatto è certamente incluso quello della sanità. Particolare attenzione è dunque rivolta all'analisi dei sistemi c.d. "ad alto rischio" (per la salute e la vita umana) e degli obblighi gravanti sugli operatori; nonché alla coerenza del nuovo quadro regolatorio con norme che disciplinano ambiti affini (Sarah Lattanzi). Un altro settore particolarmente sensibile è infine quello della giustizia, con conseguente qualificazione coma "ad alto rischio" delle applicazioni di IA che vengono utilizzate in tale ambito. Come in tutti i contesti, anche nell'amministrazione della giustizia l'IA può apportare innegabili benefici sempreché sia assicurato il rispetto dei principi di supervisione umana, trasparenza e non discriminazione (Angela Correra).

4. Il Volume è il frutto di uno sforzo congiunto da parte di giovani studiosi che nel dimostrare interesse e curiosità verso un quadro regolatorio di cosi ampia portata e certamente innovativo (da più punti di vista!) hanno saputo affrontare i vari temi dimostrando non solo di analizzare, con un approccio critico, il contenuto e la portata della nuova regolamentazione (evidenziandone pregi e lacune) ma anche di esaminare tale fonte alla luce dei principi e dei valori del diritto dell'Unione europea, e di saper altresì cogliere le implicazioni che la nuova fonte normativa può potenzialmente generare dal punto di vista istituzionale, dei rapporti tra le istituzioni, e tra ordinamenti, nonché nel ruolo che l'Unione può assumere nel contesto internazionale.

È fuor di dubbio che il Regolamento IA – come del resto accaduto per altri fonti normative quali il GDPR, il DMA, il DSA e altri ancora – susciti, per la sua portata e per la trasversalità, dibattiti sotto svariate angolature giuridiche. Lo dimostrano la numerosità degli studi (anche di particolare pregio) sulla regolazione dei sistemi di IA, condotti in questi ultimi anni nelle diverse aree giuridiche e che ne analizzano l'impatto nell'ordinamento interno con un approccio che muta a seconda delle varie sensibilità (privatistica, penalistica, costituzionalistica, amministrativistica, ecc.). L'utilizzo dei sistemi di IA è infatti in grado di rivoluzionare tutti gli ambiti della vita sociale ed economica di uno Stato, dal funzionamento della giustizia, all'erogazione dei servizi, alla responsabilità civile dei produttori e prestatori, ai mezzi di

informazione, al rapporto tra la PA e i cittadini, al mondo del lavoro, alla concorrenza tra le imprese (a tale proposito si veda il recentissimo *Digital Competition Communiqué*, adottato nell'ambito del *G7 Italia Competition Authorities and Policymakers' Summit* del 4 ottobre 2004).

È però d'altra parte incontestabile che il Regolamento resta una fonte di diritto dell'Unione europea ed è in particolare alla luce di tale ordinamento - il quale si caratterizza per una sua autonomia - che tale fonte è interpretata, apprezzata o anche criticata, per quanto riguarda i principi sui quali si fonda e a cui si ispira (Trattati, Carta dei diritti fondamentali, principi generali), gli effetti giuridici che produce, gli obblighi che pone in capo non solo ai soggetti privati ma anche agli Stati (con conseguente applicazione dei principi in materia di responsabilità nei casi di violazione), il bilanciamento tra i vari diritti in gioco (che il Regolamento ha già effettuato *ex ante*), i poteri delle istituzioni (*in primis* la Commissione) o di altri organismi pubblici e privati, i rapporti con gli ordinamenti interni e con le normative nazionali e il coordinamento con altre fonti di diritto internazionale. Sotto tale ultimo profilo, si tenga peraltro in considerazione che l'Unione europea potrebbe aderire alla Convenzione Quadro sull'IA del Consiglio d'Europa (Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,* Vilnius, 5.IX.2024), e questo potrebbe peraltro avvenire anche in un momento antecedente all'adesione alla CEDU.

5. A rimarcare l'appartenenza di tale fonte all'ordinamento europeo, non va certamente dimenticato il ruolo che la Corte di giustizia potrà svolgere per garantirne non solo un'uniformità di interpretazione e di applicazione nello spazio europeo, ma anche per valutare la rispondenza di tale atto ai valori e principi di diritto dell'Unione europea.

Va peraltro considerato che il Regolamento lascia senz'altro dei margini interpretativi non indifferenti, nonostante il chiaro intento di introdurre una disciplina chiara e dettagliata. Va da sé, infatti, che la stessa definizione di "*sistema di intelligenza artificiale*" è stata redatta cercando di contemperare l'esigenza dell'univocità e della chiarezza al fine di garantire la certezza del diritto, con quella di mantenere «la flessibilità necessaria per agevolare i futuri sviluppi tecnologici». (Relazione illustrativa al Regolamento). Le difficoltà nel precisare tale nozione (e nel farlo in maniera corretta) sono state evidenti, mancando a livello globale una definizione univoca di "sistema di intelligenza artificiale". In tale contesto preme solo evidenziare lo sforzo condotto in sede europea per rendere tale nozione il più possibile in linea con quella adottata anche a livello internazionale. Ci riferiamo in

particolare al Consiglio d'Europa, il quale, nella Convenzione Quadro recentemente adottata, ha espressamente inserito la seguente definizione: «*artificial intelligence system" means a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment*».

Il Regolamento sulla regolazione dell'IA lascia inoltre, e indubitabilmente, un certo spazio di discrezionalità agli stessi Stati membri da un punto di vista sia procedurale - dall'adozione di norme per l'adeguamento dei rispettivi ordinamenti nazionali, all'organizzazione della *governance* e dell'*enforcement* e alla designazione delle autorità competenti, all'individuazione delle sanzioni - sia sostanziale, ovvero riguardo ad alcune valutazioni che gli Stati, seppur in via eccezionale, restano liberi di effettuare Infatti, il Regolamento consente agli Stati membri, in taluni casi, di poter autorizzare, in via legislativa o amministrativa (a seconda dei casi), l'utilizzo di talune applicazioni (si veda ad esempio l'art. 5, par. 5, in relazione all'uso di sistemi di riconoscimento biometrico "*in real time*" in spazi accessibili al pubblico a fini di attività di contrasto; o l'art. 46 che consente di autorizzare - in deroga all'articolo 43 e cioè alla procedura di certificazione - l'immissione sul mercato di taluni sistemi di IA ad alto rischio, per motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente e dei principali beni industriali e infrastrutturali).

Sotto tutti questi profili la Corte avrà dunque modo, specie nel caso di rinvii pregiudiziali, di apprezzare il corretto adeguamento da parte degli Stati membri e/o il superamento dei limiti dei margini di discrezionalità concessi dal Regolamento. Questioni particolari possono porsi nel caso di interventi nazionali che intendano elevare lo *standard* di tutela dei diritti richiamando il proprio ordinamento costituzionale.

La Corte potrebbe essere inoltre chiamata a esaminare quei comportamenti statali che si situino fuori dal campo di applicazione del Regolamento, come ad esempio i provvedimenti adottati ai fini di sicurezza e difesa nazionale, ma che non dispensano, come da giurisprudenza costante, gli Stati membri dal rispetto del diritto dell'Unione.

Non meno importante sarà poi il compito della Corte di valutare rapporti e intersezioni tra il Regolamento sull'IA e gli altri regolamenti o direttive che insistono su settori limitrofi e che ipoteticamente possono coin-

volgere medesimi operatori. Implicazioni particolari potranno ad esempio aversi con riferimento al cumulo delle sanzioni e all'eventuale rispetto del principio del *ne bis in idem.*

Da ultimo, assumeranno un sicuro rilevo (anche in vista dell'adesione dell'Unione europea alla CEDU) i rapporti tra la Corte di giustizia e la Corte di Strasburgo e l'influenza della giurisprudenza di quest'ultima. Pur senza menzionare direttamente i sistemi di intelligenza artificiale (se non in limitatissimi casi, v. *Sigurdur Einarsson and others v. Iceland,* ric. n. 39757/15), la Corte EDU ha già, in una serie di sentenze, puntualizzato che lo sviluppo tecnologico, e il conseguente rischio di una maggiore lesività dei diritti dell'uomo causato dall'utilizzo di talune applicazioni, impongono allo Stato una responsabilità particolare, e ne rafforzano l'obbligo di introdurre adeguate garanzie e idonei rimedi all'interno del proprio ordinamento.

Alla luce delle tante questioni che si sono già poste e delle altre che certamente sorgeranno, l'augurio (e la speranza) è dunque che questo Volume - che già esamina con molta attenzione e chiarezza una nutrita serie di problematiche - possa suscitare ulteriore interesse tra gli studiosi, giovani ma anche meno giovani, su un tema che è sì certamente tecnico ma che riflette le specificità e allo stesso tempo genera ricadute importanti per l'ordinamento e il diritto dell'Unione europea.

Introduzione

di *Federico Ferri*

"Oggi sembra impossibile liberarsi della pressione di altre discipline, che vorrebbero estendersi e talvolta appropriarsi all'insegnamento del diritto dell'Unione. Ma allora era esattamente il contrario: si trattava di attirare l'attenzione sul processo d'integrazione europea e sulla disciplina che lo studiava a fronte del disinteresse e dello scetticismo dei più".

Queste parole sono state pronunciate quasi un anno fa dal Prof. Antonio Tizzano, nel Discorso tenuto in occasione del conferimento del Dottorato *ad honorem* da parte dell'Università di Padova. Si riferiscono alle fasi iniziali della sua attività e sono ora riportate nel fascicolo speciale di questa Rivista che raccoglie gli Atti del V Convegno Nazionale AISDUE, intitolato "Il Diritto dell'Unione europea nei rapporti tra ordinamenti: tra collaborazione, integrazione e identità" (p. 40).

Ebbene, tali parole fungono da filo rosso (ovviamente involontario) per lo sviluppo del lavoro risultante dall'impegno assunto da chi ha contribuito alla realizzazione di questo ulteriore numero speciale della Rivista, avente ad oggetto il Regolamento UE sull'intelligenza artificiale e pensato durante una riunione del comitato di redazione del *BlogDUE*. È, infatti, all'interno di esse che possono essere rinvenuti il fulcro e l'ambizione dell'opera.

Il fulcro è rappresentato da un'espressione per certi versi antica, ma al tempo stesso estremamente moderna: "integrazione europea". Come si situa una riforma di portata e proporzioni così vaste nell'ampio contesto del processo di integrazione europea? Questa la domanda di fondo attorno alla quale ruotano i profili di indagine delle studiose e degli studiosi che, individualmente e nel loro insieme, hanno cercato di fornire qualche risposta e, soprattutto, di alimentare interrogativi per nuovi (o rinnovati) spunti di riflessione.

L'ambizione, invece, consiste nel mettere a sistema, di fronte ad una simile sfida, frammenti di conoscenza prodotti nell'ambito della medesima disciplina, ossia quella che, ricollegandosi alle parole del Prof. Tizzano, studia il processo d'integrazione europea. Ciò al fine di cogliere un'occasione propizia per creare una prospettiva di osservazione comune e interna rispetto a uno strumento di diritto dell'Unione che inevitabilmente cattura – e catturerà – l'attenzione di esponenti di molte altre discipline, talvolta addirittura

estranee all'area giuridica. Il tutto, si badi bene, non certo in un'ottica di isolamento, ma nel tentativo di favorire il prodursi di condizioni favorevoli per un più efficace confronto tra saperi, al servizio dell'integrazione europea e dei beneficiari di questo processo.

Pertanto, l'auspicio è che il presente fascicolo non sia percepito soltanto come la chiusura di un percorso, bensì come un punto di passaggio, posizionato lungo quella che può essere intesa come una traiettoria in continuo divenire: metafora, quest'ultima, che si addice non solo all'evoluzione dell'intelligenza artificiale, ma anche…al processo d'integrazione europea.

L'occasione è gradita per porgere i più sentiti ringraziamenti alle Autrici e agli Autori dei vari articoli del fascicolo speciale, alle Maestre e ai Maestri che hanno supervisionato i lavori, in particolare la Prof.ssa Cristina Schepisi, e infine al Prof. Antonio Tizzano, alla Prof.ssa Patrizia De Pasquale e al Prof. Fabio Spitaleri, per avere reso possibile questa avventura.

Articoli

INTELLIGENZA ARTIFICIALE E PRINCIPIO DEMOCRATICO: RIFLESSIONI A MARGINE DELL'EMERSIONE DI UN QUADRO NORMATIVO EUROPEO

Giovanni Zaccaroni[*]

SOMMARIO: 1. Introduzione. – 2. La risoluzione delle Nazioni Unite su «*safe, secure and trustworthy artificial intelligence systems for sustainable development*». – 3. La Convenzione quadro del Consiglio d'Europa su intelligenza artificiale, diritti umani, democrazia e Stato di diritto. – 3.1. La definizione di IA e l'ambito di applicazione della Convezione – 3.2. Gli obblighi generali ed i principi applicabili all'IA. – 3.3. Il meccanismo di gestione del rischio. – 3.4. Il ruolo dell'Unione europea nella Convenzione quadro. – 4. Il regolamento sull'intelligenza artificiale, la gestione del rischio ed il principio democratico. – 4.1. I riferimenti al principio democratico ed ai diritti fondamentali nella parte introduttiva del regolamento. – 4.2. La gestione del rischio e la valutazione di impatto in materia di diritti fondamentali. – 5. Il *Media Freedom Act*, il *Digital Services Act* ed i profili applicabili alla tutela del principio democratico. – 5.1. Il *Media Freedom Act.* – 5.2. Il *Digital Services Act*. – 6. Conclusione.

1. *Introduzione*

Il principio democratico (oppure, come recitano in maniera più incisiva i Trattati, i "principi" democratici[1]) è uno dei principi che fondano la vita istituzionale dell'Unione europea[2], nonché uno dei valori su che ispirano la sua azione[3]. La ragione per cui ci si riferisce ad una pluralità di princi-

[*] Ricercatore a tempo determinato in diritto dell'Unione europea, Dipartimento di Giurisprudenza, Università degli Studi di Milano-Bicocca – giovanni.zaccaroni@unimib.it.

[1] Per semplicità, e salvo diversa indicazione, quando in questo scritto l'Autore menziona il principio democratico intende i "principi" democratici così come definiti nei Trattati e descritti nel paragrafo di seguito.

[2] Su cui v. K. LENAERTS, *The principle of democracy in the case law of the Court of Justice*, in *ICLQ*, 2013, p. 271 ss. M.E. BARTOLONI, *Il principio democratico rappresentativo nella giurisprudenza della Corte di giustizia. Il deficit democratico dell'UE è una premessa necessaria?* in *I Post AISDUE,* I, 2019, p. 32 ss., www.aisdue.eu/maria-eugenia-bartoloni-il-principio-democratico-rappresentativo-nella-giurisprudenza-della-corte-di-giustizia-il-deficit-democratico-dellue-e-una-premessa-necessaria/.

[3] Art. 2 TUE. La distinzione tra il "valore" democratico ed il "principio" democratico è ripresa anche nel Preambolo al Trattato di Lisbona, dove si legge dapprima che gli Stati

pi è probabilmente da ricercarsi nello sfortunato ma ambizioso progetto di Trattato Costituzione[4]. Tale Trattato, infatti, nel Titolo VI distingueva tra tre diversi principi democratici[5]. Il principio dell'uguaglianza democratica, secondo cui le istituzioni dell'Unione dedicano uguale attenzione ai cittadini degli Stati membri[6]. Il principio della democrazia rappresentativa, che si riflette nella possibilità dei cittadini di eleggere e di essere eletti quali membri del Parlamento europeo[7]. Ed il principio della democrazia partecipativa[8], che prevede la possibilità, per i cittadini e per le relative forme di espressione della vita democratica, quali le associazioni rappresentative degli interessi dei cittadini e la società civile, di partecipare in maniera attiva al lavoro delle istituzioni in varie modalità che il Trattato Costituzione elencava negli artt. successivi. Tra di esse ricordiamo l'iniziativa dei cittadini europei, il dialogo sociale, l'accesso al mediatore europeo e la trasparenza, nonché la protezione dei dati di carattere personale ed il dialogo con le confessioni religiose[9].

Con il Trattato di Lisbona, invece, a seguito delle ormai note vicende legate alla mancata ratifica del Trattato Costituzione, i tre "principi" democratici vengono inseriti all'inizio del Trattato sull'Unione europea (TUE)[10].

Il principio dell'uguaglianza dei cittadini viene inserito all'art. 9 del TUE, dove viene incluso anche il riferimento alla cittadinanza dell'Unione

membri «Ispirandosi alle eredità culturali, religiose e umanistiche dell'Europa, da cui si sono sviluppati i valori universali […] della democrazia, dell'uguaglianza e dello Stato di diritto […]» e successivamente che «Confermando il proprio attaccamento ai principi […] della democrazia e del rispetto dei diritti dell'uomo e delle libertà fondamentali nonché dello Stato di diritto […]».

[4] K. Lenaerts, P. van Nuffel, *EU Constitutional Law*, Oxford, 2022, p. 43.

[5] Sul Trattato Costituzione v. L.S. Rossi (a cura di), *Il progetto di trattato-costituzione. Verso una nuova architettura dell'Unione europea*, Milano, 2004.

[6] Trattato Costituzione, art. I-45.

[7] Trattato Costituzione, art. I-46.

[8] Trattato Costituzione, art. I-47.

[9] Trattato Costituzione, artt. da I-48 a I-52.

[10] Il Trattato Costituzione avrebbe dovuto entrare il vigore a seguito della ratifica negli Stati membri. In Francia e nei Paesi Bassi sono stati indetti e si sono tenuti referendum per autorizzare la ratifica, con esito sfavorevole. In Danimarca, Irlanda, Portogallo, Polonia, Regno Unito e Repubblica Ceca, il referendum avrebbe potuto comunque avere luogo sia per autorizzare che per confermare la ratifica del Trattato Costituzione. Si veda lo studio della Camera dei Deputati sul Trattato Costituzione, disponibile al *link*: leg15.camera.it/cartellecomuni/leg14/RapportoAttivitaCommissioni/testi/14/14_cap05_sch02.htm#:~:text=La%20ratifica%20del%20Trattato%20costituzionale,%2C32%25%20ha%20votato%20s%C3%AC.&text=Il%20disegno%20di%20legge%20di,Bundestag%20il%2012%20maggio%202005.

europea. All'art. 10, invece, vengono riassunti i vecchi testi degli artt. I-46 ed I-47 del Trattato Costituzione. I paragrafi 1 e 2 dell'art. 10 si riferiscono alla democrazia rappresentativa, ed i paragrafi 3 e 4 alla democrazia partecipativa. Buona parte, invece, di quegli istituti tipici della democrazia partecipativa più sopra descritti (come il dialogo con i cittadini e le associazioni rappresentative e l'obbligo di consultazioni pubbliche da parte della Commissione europea) tra cui svetta certamente l'iniziativa dei cittadini europei[11], vengono concentrati nel testo dell'attuale art. 11 del TUE[12]. I restanti istituti vengono dispersi nel testo dei Trattati[13].

Dunque, il quadro stabilito dai Trattati crea in capo alle istituzioni un obbligo giuridico di utilizzare il principio democratico e di promuoverlo nelle sue politiche, non solo come valore ma anche come principio che costituisce e caratterizza il metodo dell'Unione europea.

È in virtù, dunque, del ruolo specifico che il principio democratico riveste nell'ordinamento dell'Unione europea che bisogna prestare particolare attenzione alle conseguenze che possono derivare nei suoi confronti dall'utilizzo e dall'applicazione delle innovazioni tecnologiche; ed è vero anche il contrario, perché l'approccio alla regolamentazione dell'innovazione tecnologica può condizionare la democrazia[14].

Se in un primo momento, infatti, sembrava che l'utilizzo dell'innovazione tecnologica potesse rappresentare un'occasione per aumentare la partecipazione dei cittadini al processo democratico (europeo ma anche e soprattutto nazionale)[15], è poi apparso gradualmente chiaro che l'utilizzo della

[11] Su cui v. A. Santini, *L'iniziativa dei cittadini europei. Quale contributo alla legittimità democratica dell'Unione?* Napoli, 2019; M. Inglese, *L'iniziativa dei cittadini europei a dieci anni dal Trattato di Lisbona: tra consolidate criticità e inesplorate prospettive*, in *federalismi.it*, 2020, p. 194 ss.

[12] Sulla democrazia partecipativa nel quadro del Trattato di Lisbona v. G. Morgese, *Principio e strumenti della democrazia partecipativa nell'Unione europea* in E. Triggiani (a cura di), *Le nuove frontiere della cittadinanza europea*, Bari, 2011, p. 37 ss.

[13] Il dialogo con le confessioni religiose e le organizzazioni non confessionali è attualmente previsto all'art. 17 del TFUE, mentre il Mediatore europeo è menzionato agli artt. 20, 24 e disciplinato all'228 del TFUE. Senza poi dimenticare che buona parte di essi vengono menzionati anche nella Carta dei diritti fondamentali dell'Unione europea, nel Titolo IV (Cittadinanza) agli artt. 41 (Diritto ad una buona amministrazione), 42 (Diritto di accesso ai documenti) e 43 (Mediatore europeo).

[14] V. l'interessante tesi dottorale di M. Klang, *Disruptive Technology. Effects of Technology Regulation on Democracy*, Gothenburg Studies in Informatics, n. 36, 2006, gupea.ub.gu.se/handle/2077/9910.

[15] V. in senso critico R. Pagano, *Telematica e democrazia diretta,* in *Rivista di Informatica e Diritto*, n. 3, 1984, p. 27 ss., in particolare a p. 28.

tecnologia andava piuttosto controllato[16]. Se tale ragionamento è valido con una tecnologia che ha certamente cambiato il modo con cui l'individuo si relaziona con la politica e l'organizzazione democratica come il World Wide Web[17], è però ancora più importante con una tecnologia come l'intelligenza artificiale che, insieme a molteplici opportunità, può creare anche molti problemi alla struttura dell'ordinamento democratico[18].

In virtù delle specifiche caratteristiche del principio democratico nell'ordinamento dell'Unione europea, tale principio tende a spostarsi in maniera consistente verso la democrazia rappresentativa, che è citata direttamente come "fondamento" dell'Unione europea all'art. 10 TUE[19]. Tecnologie che possono disintermediare o comunque ridurre la distanza tra la politica ed i cittadini, come l'intelligenza artificiale, devono essere considerate con attenzione per evitare che il funzionamento democratico venga compromesso in tutto o in parte.

Per essere più concreti, si pensi a questo esempio: una piattaforma online utilizza un algoritmo di intelligenza artificiale che seleziona, sulla base della cronologia delle visualizzazioni, i contenuti che ritiene più adatti all'utente. Se tale utente, dunque, è interessato prima di tutto all'ambiente ed all'ecologia (per fare un esempio innocuo) vedrà soprattutto contenuti di questo tenore. Pensiamo poi che, per assurdo, la società che possiede la piattaforma online abbia interessi nel mercato delle energie rinnovabili e che, per questo, cominci a modificare l'algoritmo per mostrare video che promuovono la sostenibilità dei veicoli elettrici e perfino, con l'approssimarsi di una scadenza elettorale, cominci a mostrare i contenuti di un politico che si spende attivamente per l'utilizzo dei motori elettrici al posto di quelli a combustione (ma potrebbe essere il contrario).

L'utilizzo dell'intelligenza artificiale, infatti, permette agli sviluppatori

[16] S. Rodotà, *Tecnologie e Diritti*, Bologna, 2021. Il volume, pubblicato per la prima volta nel 1995, è stato poi ripubblicato più volte, da ultimo nel 2021 (a cura degli allievi, successivamente alla morte dell'Autore). Alle pp. 124 e 125 l'Autore menziona infatti proprio il tentativo di Newt Gingrich di proporre un "Congresso virtuale" degli Stati uniti e dunque fare a meno dei rappresentanti eletti.

[17] Il funzionamento della tecnologia che compone World Wide Web è ispirato ai principi della democrazia partecipativa. Per esempio, una delle organizzazioni internazionali più influenti ed importanti per il suo funzionamento, la *Internet Society*, è regolata da un sistema di democrazia partecipativa.

[18] P. Nemitz, *Constitutional democracy and technology in the age of artificial intelligence,* in *Philosophical Transactions of the Royal Society A,* 2018, p. 1 ss.

[19] Art. 10, par. 1: «Il funzionamento dell'Unione si fonda sulla democrazia rappresentativa».

ed ai fornitori di questi servizi di processare una vasta quantità di dati ed attraverso di essi di prevedere, seppure con qualche approssimazione, i gusti, desideri e comportamenti dei cittadini elettori, fino ad influenzare direttamente o indirettamente il processo elettorale[20].

Per mitigare i rischi che possono insorgere per l'ordinamento democratico dallo sviluppo e dalla commercializzazione dell'intelligenza artificiale è però difficile guardare soltanto all'Unione europea. È invece utile rivolgere lo sguardo oltre, e riflettere su altri tentativi, fatti da organizzazioni internazionali, anche a carattere regionale, per cominciare a lavorare sui problemi e sulle opportunità poste dall'intelligenza artificiale.

Proprio per questo, il contributo prenderà dapprima in esame la recente risoluzione delle Nazioni Unite sull'intelligenza artificiale[21], per poi continuare con l'analisi dell'innovativa Convenzione promossa dal Consiglio d'Europa su intelligenza artificiale, Stato di diritto e democrazia[22], finendo poi con la disciplina rilevante dell'Unione europea, tra cui l'analisi del meccanismo di gestione del rischio per i diritti fondamentali nel regolamento sull'intelligenza artificiale (*AI Act*)[23] e l'analisi delle disposizioni rilevanti applicabili ai mezzi di comunicazione (*Media Freedom Act*)[24] e alle piattaforme digitali (*Digital Services Act*)[25].

L'obiettivo di questo scritto è dunque capire se sta davvero emergendo un quadro giuridico europeo (e non solo, visto il riferimento alla risoluzione delle Nazioni Unite) che possa prevenire e contrastare le potenziali minacce

[20] Tutto questo, peraltro, considerando che gli attori che potrebbero interferire con il processo democratico siano mossi soltanto da motivazioni di natura economica. Qualora, invece, i motivi siano di natura sociale o addirittura politica (per esempio, promuovere il passaggio ad una forma di governo meno democratica) la situazione potrebbe persino peggiorare.

[21] Risoluzione dell'Assemblea Generale delle Nazioni Unite del 21 marzo 2024, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, undocs.org/Home/Mobile?FinalSymbol=A%2F78%2FL.49&Language=E&DeviceType=Desktop&LangRequested=False.

[22] Consiglio d'Europa, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,* www.coe.int/en/web/artificial-intelligence/cai.

[23] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale [*AI Act*]. I riferimenti successivi all'*AI Act* si intendono fatti a questo testo.

[24] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno [*Media Freedom Act*].

[25] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali [*Digital Services Act*].

che provengono da un utilizzo scorretto dell'intelligenza artificiale sull'ordinamento democratico senza compromettere eccessivamente l'innovazione.

2. *La risoluzione delle Nazioni Unite su* «safe, secure and trustworthy artificial intelligence systems for sustainable development»

L'Organizzazione delle Nazioni Unite ha cominciato ad affrontare il tema dell'intelligenza artificiale solo di recente, rispetto ad altre organizzazioni internazionali[26]. L'istituzione di un *High-Level Advisory Body on Artificial Intelligence*, per esempio, è arrivata nel 2023, e si concluderà con una relazione che dovrebbe essere pubblicata nella seconda parte del 2024[27].

Questo ritardo, però, pare forse legato più all'ampio spettro di competenze e di ruoli che le Nazioni Unite rivestono nell'ordinamento internazionale che a ragioni di opportunità, poiché in realtà è da tempo che si discute dell'applicabilità del diritto internazionale convenzionale all'intelligenza artificiale[28].

Tuttavia, e non senza una certa tempestività, l'Assemblea Generale delle Nazioni Unite ha presentato ed approvato, nella sessione dell'11 marzo 2024, una risoluzione sull'intelligenza artificiale che probabilmente[29] apre la strada all'adozione di una vera e propria convenzione internazionale sul tema[30].

[26] Come, ad esempio, il Consiglio d'Europa. V. *infra*, par. 3. Bisogna però dire che alcune riflessioni, seppure non ufficiali, erano già disponibili sui canali di comunicazioni delle Nazioni Unite. V. per esempio E. Pauwels, *How Can Multilateralism Survive the Era of Artificial Intelligence?*, in *UN Chronicles*, 2018, www.un.org/en/chronicle/article/how-can-multilateralism-survive-era-artificial-intelligence.

[27] Nazioni Unite, *High-Level Advisory Body on Artificial Intelligence*. Più informazioni sono disponibili al link: www.un.org/techenvoy/ai-advisory-body.

[28] V. P. Čerka, J. Grigienė, G. Sirbikytė, *Liability for damages caused by artificial intelligence*, in *Computer Law & Security Review*, n. 3, 2015, p. 376 ss., dove si discute dell'applicabilità all'intelligenza artificiale dell'art. 12 della Convenzione delle Nazioni Unite sull'uso delle comunicazioni elettroniche nei contratti internazionali del 23 novembre 2008. Oppure più generalmente sulla necessità di un dibattito in seno alle Nazioni Unite sull'intelligenza artificiale v. K. J. Smith, *The AI Community and the United Nations: A Missing Global Conversation & A Closer Look at Social Good,* in *Association for Advancement of Artificial Intelligence (AAAI) Spring Symposium Series*, 2017, cdn.aaai.org/ocs/15387/15387-68202-1-PB.pdf.

[29] M. Francisco, B. Linnér, *AI and the governance of sustainable development. An idea analysis of the European Union, the United Nations, and the World Economic Forum*, in *Environmental Science & Policy*, 2023, www.sciencedirect.com/science/article/pii/S1462901123002393.

[30] E. Fournier-Tombs, *Towards a United Nations Internal Regulation for Artificial Intelligence*, in *Big Data & Society*, 2021, p. 1 ss.

Vale dunque la pena soffermarsi sui contenuti di questa risoluzione, per capire come l'approccio seguito dalle Nazioni Unite si caratterizza rispetto a quello perseguito dall'Unione europea e dal Consiglio d'Europa, che vedremo nei prossimi paragrafi.

Il primo elemento degno di nota è che la risoluzione è di un tenore decisamente più ampio rispetto allo scopo di questo scritto, che, come detto, si concentra sul principio democratico[31]. Però, proprio perché nel titolo viene chiamata in causa l'Agenda 2030 per lo sviluppo sostenibile[32], non si può non considerare come l'Agenda stessa menzioni da un lato la democrazia (insieme allo Stato di diritto) come elementi essenziali dello sviluppo sostenibile[33]. Inoltre, l'Obiettivo n. 16 dell'Agenda 2030 è intitolato «Promuovere società pacifiche e inclusive per uno sviluppo sostenibile, garantire a tutti l'accesso alla giustizia, e creare istituzioni efficaci, responsabili ed inclusive a tutti i livelli»[34] ed al punto 16.3, ancora più chiaramente, enuncia che uno degli obiettivi secondari dell'Agenda 2030 è «Promuovere lo Stato di diritto a livello nazionale e internazionale e garantire un pari accesso alla giustizia per tutti». Dunque, il rispetto del principio democratico, benché non espresso apertamente, è richiamato dalla risoluzione attraverso la menzione dello Stato di diritto e dell'Obiettivo n. 16 nell'Agenda 2030.

Il secondo elemento interessante è che la risoluzione menziona come ambito di applicazione (nello stesso modo in cui fa la Convenzione quadro del Consiglio d'Europa) il concetto di "ciclo di vita" (*life cycle*) dell'intelligenza artificiale[35]. Tale "ciclo di vita" include una serie di passaggi, che vanno dalla fase iniziale di preparazione e programmazione, fino alla sua vendita ed eventuale dismissione: «pre-design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning»[36].

Sempre secondo la risoluzione, gli elementi che compongono il ciclo

[31] Considerazione abbastanza immediata, che si ottiene dal titolo «Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development».

[32] Risoluzione adottata dall'Assemblea Generale il 25 settembre 2015, *Trasformare il nostro mondo: l'Agenda 2030 per lo Sviluppo Sostenibile,* unric.org/it/wp-content/uploads/sites/3/2019/11/Agenda-2030-Onu-italia.pdf.

[33] *Ibidem*, p. 4.

[34] *Ibidem*, p. 25.

[35] Risoluzione dell'Assemblea Generale delle Nazioni Unite del 21 marzo 2024, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, cit. a p. 2.

[36] *Ibidem.*

di vita dell'intelligenza artificiale devono mettere l'essere umano al centro, essere affidabili, etici, inclusivi e pensati per assicurare il massimo rispetto e la promozione dei diritti fondamentali e del diritto internazionale, nonché proteggere la riservatezza, orientati allo sviluppo sostenibile e responsabili[37].

La risoluzione, poi, riconosce anche che lo sviluppo e l'utilizzo improprio dell'intelligenza artificiale può rinforzare i pregiudizi, le diseguaglianze e le discriminazioni, nonché mettere a repentaglio la protezione e la promozione dei diritti e delle libertà fondamentali, incluso il diritto a non essere sottoposti ad arbitrarie interferenze della propria riservatezza[38].

Ma il punto più interessante, quantomeno ai fini dalla presente trattazione, è il par. n. 5, dove l'Assemblea Generale invita gli Stati membri a rispettare i diritti fondamentali nel corso di tutto il ciclo di vita dell'intelligenza artificiale, nonché a cessare l'utilizzo di tutti quei sistemi di intelligenza artificiale che non possono operare rispettando i diritti fondamentali così come riconosciuti dall'ordinamento internazionale, riaffermando dunque che i diritti di cui le persone godono (o dovrebbero godere) nel mondo reale devono continuare anche nella dimensione *online*[39]. La notazione della continuità tra lo spazio online e quello offline non è di poco conto, poiché afferma – probabilmente per la prima volta in sede internazionale, quantomeno con riferimento all'intelligenza artificiale – il principio secondo il quale l'ordinamento reale e quello digitale sono distinti, ma che i principi

[37] *Ibidem*, p. 2, dove sono elencate le caratteristiche del ciclo di vita dell'intelligenza artificiale che sono state sopra liberamente tradotte dall'Autore a beneficio del Lettore: «human-centric, reliable, explainable, ethical, inclusive, in full respect, promotion and protection of human rights and international law, privacy preserving, sustainable development oriented, and responsible».

[38] *Ibidem*, p. 3: «[I]mproper or malicious design, development, deployment and use of artificial intelligence systems, such as without adequate safeguards or in a manner inconsistent with international law, pose risks that could hinder progress towards the achievement of the 2030 Agenda for Sustainable […] reinforce structural inequalities and biases; lead to discrimination; […] undercut the protection, promotion and enjoyment of human rights and fundamental freedoms, including the right not to be subject to unlawful or arbitrary interference with one's privacy».

[39] *Ibidem,* p. 5, par. 5: «Emphasizes that human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, calls upon all Member States and, where applicable, other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, especially of those who are in vulnerable situations, and reaffirms that the same rights that people have offline must also be protected online, including throughout the life cycle of artificial intelligence systems».

fondamentali che governano un ordinamento governano anche l'altro[40].

Un altro elemento che può rappresentare un ponte tra gli strumenti che le Nazioni Unite e le altre organizzazioni internazionali e sovranazionali stanno approvando per regolare l'intelligenza artificiale è senza dubbio il riferimento alla gestione del rischio e alla valutazione dell'impatto sui diritti fondamentali[41]. La risoluzione infatti, cita due strumenti che rappresentano elementi molto importanti sia nella Convenzione quadro del Consiglio d'Europa che nel regolamento dell'Unione europea sull'intelligenza artificiale.

La risoluzione dell'Assemblea Generale delle Nazioni Unite, dunque, a una prima lettura, sembra potere far parte a pieno titolo di un potenziale quadro che sta emergendo a tutela del principio democratico e, più in generale, dei diritti fondamentali nell'ambito dell'innovazione tecnologica e dell'intelligenza artificiale. Tuttavia, qualora questo sforzo non guidi, in ultima analisi, ad una Convenzione che garantisca livelli quantomeno comparabili di tutela per gli utilizzatori dei sistemi di intelligenza artificiale nei differenti ordinamenti, è piuttosto probabile che, a livello globale, si rinsaldino "isole" (come l'Unione europea) dove la regolamentazione dell'innovazione tecnologica e la tutela dei diritti è più severa, circondate da un "mare" dove invece la sperimentazione dell'innovazione è liberamente permessa, ma dove potrebbero esserlo anche le violazioni del principio democratico e dei diritti fondamentali.

3. *La Convenzione quadro del Consiglio d'Europa su intelligenza artificiale, diritti umani, democrazia e Stato di diritto*

Lo spazio giuridico europeo, come già ben noto, è caratterizzato dalla coabitazione, sin dagli inizi, tra un'organizzazione sovranazionale inizialmente a carattere principalmente economico (che è poi diventata l'Unione europea) ed un'altra che invece ha nella sua vocazione la tutela dei diritti

[40] Tale concetto si può riassumere con quello di sovranità digitale, su cui si rimanda, tra gli altri, a F. Ferri, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Torino, 2023, che, a p. 45 lo cita con riferimento alla dimensione esterna dell'Unione. Per una ulteriore ed aggiornata ricostruzione del concetto, v. anche E. Celeste, *Digital constitutionalism, EU digital sovereignty ambitions and the role of the European declaration on digital right*s in *REBUILD Centre Working Paper*, 2024 ssrn.com/abstract=4698091.

[41] Risoluzione dell'Assemblea Generale delle Nazioni Unite del 21 marzo 2024, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, cit. a p. 6, lettera (l).

fondamentali (il Consiglio d'Europa). Le strade intraprese dai due ordinamenti si sono poi incrociate molte volte, e più volte è stata tentata l'adesione dell'Unione europea ad una delle Convenzioni di maggior successo promosse dal Consiglio d'Europea, la Convenzione europea dei diritti dell'uomo (CEDU).

Il Consiglio d'Europa, nonostante il momento di grave crisi istituzionale[42], ha preceduto, anche se non di molto, l'Unione europea nell'attenzione dedicata al rapporto tra nuove tecnologie e diritti fondamentali, con particolare riferimento al principio democratico[43]. Tale lavoro è culminato nella recentissima adozione ed apertura alla firma di una Convenzione quadro su intelligenza artificiale, diritti umani, democrazia e Stato di diritto (Convenzione quadro), primo strumento di diritto internazionale ad occuparsi dell'impatto delle nuove tecnologie sull'ordinamento democratico[44]. Tale Convenzione, al momento della pubblicazione di questo scritto, è stata firmata (ma ancora non ratificata) da Andorra, Georgia, Islanda, Norvegia, Moldavia, San Marino, Regno Unito, nonché da Israele e Stati Uniti e dall'Unione europea[45].

La Convenzione quadro è il risultato di un lavoro più ampio che il Consiglio d'Europa ha cominciato a svolgere sin dal 2018, con diversi documenti pubblicati proprio sull'intelligenza artificiale ed i diritti fondamentali[46].

Il primo aspetto da ricordare è la natura di "convenzione quadro" dello strumento che il Consiglio d'Europa sta promuovendo tra gli Stati membri, che significa cioè, per stessa ammissione della commissione responsabile

[42] Per un concorrere di ragioni, tra le quali la "concorrenza" dell'Unione europea nella tutela dei diritti fondamentali e la tensione tra allargamento orizzontale (geografico) e verticale (disponibilità di strumenti giuridici per incidere sulla tutela dei diritti fondamentali. Tali tensioni sono culminate nella crisi che ha coinvolto il Consiglio d'Europa, che ha coraggiosamente marginalizzato la Federazione Russa (suo Stato membro) fin dall'inizio dell'instabilità in Ucraina, culminata con la sua espulsione nelle settimane successive all'invasione di fine febbraio 2022.

[43] Sulla competizione – positiva – per regolamentare l'IA tra Consiglio d'Europa e Unione europea, v. J. Ziller, *The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments,* in *Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, 2024, p. 202 ss.

[44] La Convenzione quadro del Consiglio d'Europa su intelligenza artificiale, diritti umani, democrazia e Stato di diritto è stata adottata il 17 maggio 2024 dal Comitato dei Ministri del Consiglio d'Europa (Sessione n. 133) ed è aperta alla firma a partire dal 5 settembre 2024.

[45] *Council of Europe opens first ever global treaty on AI for signature,* 5 settembre 2024, www.coe.int/en/web/portal/-/council-of-europe-opens-first-ever-global-treaty-on-ai-for-signature.

[46] Una lista che raccoglie gli studi e le ricerche promosse dal Consiglio d'Europa sull'intelligenza artificiale è disponibile a questo indirizzo www.coe.int/en/web/artificial-intelligence/work-in-progress#02EN.

per l'approvazione della Convenzione, che potrebbero essere adottate altre convenzioni dedicate a specifici aspetti che riguardano il rispetto dei diritti fondamentali nel ciclo di vita dell'intelligenza artificiale[47].

Come accaduto anche per la risoluzione delle Nazioni Unite già citata, infatti, il testo della Convenzione fa riferimento sin dal Preambolo alla necessità di rispettare i diritti fondamentali nel corso di tutto il ciclo di vita dell'intelligenza artificiale (IA), specificando che le varie attività che compongono tale ciclo di vita potrebbero avere un impatto profondamente positivo sulla promozione della prosperità e del benessere individuale e collettivo[48]. Subito dopo, poi, il Preambolo continua dichiarando che l'IA potrebbe dare opportunità senza precedenti per proteggere i diritti umani, la democrazia e lo Stato di diritto[49]. Questo approccio sembra partire dai vantaggi dell'applicazione dell'IA, anziché dagli svantaggi, che sono comunque prontamente elencati successivamente: il rischio di minare l'autonomia della persona, la sua dignità, i diritti umani e la democrazia, le potenziali discriminazioni e la possibilità di utilizzare l'IA per reprimere l'espressione dei diritti fondamentali[50]. Il Preambolo della Convenzione quadro cita anche l'esigenza, ripresa già dalla risoluzione delle Nazioni Unite, di stabilire un quadro giuridico globale che disciplini l'IA[51], e che rispetti e tenga conto del diritto internazionale applicabile[52].

Con riguardo al contenuto preciso della Convenzione quadro, emergono

[47] Convenzione quadro su intelligenza artificiale, diritti umani, democrazia e Stato di diritto, Preambolo: «Recognising the framework character of this Convention, which may be supplemented by further instruments to address specific issues relating to the activities within the lifecycle of artificial intelligence systems».

[48] *Ibidem,* « […] activities within the lifecycle of artificial intelligence systems, […] have the potential to promote human prosperity as well as individual and societal well-being, sustainable development, gender equality and the empowerment of all women and girls, as well as other important goals and interests, by enhancing progress and innovation».

[49] *Ibidem,* «Recognising that activities within the lifecycle of artificial intelligence systems may offer unprecedented opportunities to protect and promote human rights, democracy and the rule of law».

[50] *Ibidem,* «Concerned that certain activities within the lifecycle of artificial intelligence systems may undermine human dignity and individual autonomy, human rights, democracy and the rule of law; Concerned about the risks of discrimination in digital contexts [...]; Concerned by the misuse of artificial intelligence systems and opposing the use of such systems for repressive purposes […]».

[51] *Ibidem,* «Convinced of the need to establish, as a matter of priority, a globally applicable legal framework setting out common general principles and rules governing the activities within the lifecycle of artificial intelligence […]».

[52] *Ibidem,* «Mindful of applicable international human rights instruments, such as […]».

almeno quattro aspetti: la definizione di intelligenza artificiale ed il suo ambito di applicazione; i principi applicabili all'IA; il meccanismo di gestione del rischio, ed il ruolo riservato dalla Convenzione quadro all'Unione europea.

3.1. *La definizione di IA e l'ambito di applicazione della Convezione*

Nella Convenzione quadro, l'IA viene definita come: "a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment»[53].

Questa definizione che ha alcune caratteristiche interessanti[54]. Prima di tutto, definisce l'IA come "machine-based system", e cioè che utilizzi la potenza di calcolo di un processore per lavorare i dati che vengono forniti alla macchina. Poi, un sistema che, tramite i dati forniti, inferisca predizioni, contenuti, raccomandazioni o decisioni[55]. Dunque, anche se tale definizione sembra privilegiare la cosiddetta intelligenza artificiale generativa, che è quella più conosciuta ed utilizzata quantomeno fino ad ora, si può applicare anche ad altre situazioni[56].

Bisogna poi considerare che (terza caratteristica) i contenuti generati dall'IA possono influenzare l'ambiente fisico o virtuale[57]. Per questo, dunque, la definizione di IA – in linea con quella proposta dall'OCSE/OECD – sembra includere una vasta gamma di situazioni al suo interno, tra cui anche alcune

[53] Art. 2, Convenzione quadro.

[54] La definizione contenuta nella Convenzione quadro è sostanzialmente identica a quella data dall'OCSE/OECD (come successivamente aggiornata) e contenuta nelle *OECD Recommendation on AI* (2019). Tale definizione è stata poi aggiornata nel 2023. Su questo, si veda: *Explanatory memorandum on the updated OECD definition of an AI system*, in *OECD artificial intelligence papers*, n. 3, 2024, www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.

[55] Sul concetto di inferimento, si veda *Explanatory memorandum on the updated OECD definition of an AI system*, cit., p. 9.

[56] Lo *Explanatory memorandum on the updated OECD definition of an AI system*, cit., sempre a p. 9, esplicita l'esempio dei sistemi di guida automatica, i quali, per esempio, riconoscono come un pedone i pixel che sono collocati in una determinata regione del campo di visualizzazione di una videocamera.

[57] Questo terzo elemento non sembra essere spiegato nell'OECD Explanatory memorandum, cui rimanda anche la Commissione che ha redatto la Convenzione quadro nel suo *Explanatory Report*.

che potrebbero non essere necessariamente basate sull'intelligenza artificiale[58]. Tuttavia, pensando al ruolo della Convenzione quadro, che si rivolge a 47 Stati membri molto diversi tra di loro, la scelta di una definizione inclusiva sembra appropriata.

Riguardo invece l'ambito di applicazione, la Convenzione quadro si riferisce a tutto il ciclo di vita delle intelligenze artificiali che possono influenzare i diritti fondamentali, la democrazia e lo Stato di diritto: tali IA rientrano sia che siano utilizzate da autorità pubbliche che da soggetti privati, e le parti della Convenzione quadro dovranno dare, all'atto della firma oppure della ratifica, puntuale descrizione degli strumenti utilizzati per dare attuazione alla Convenzione[59].

Rimangono tuttavia fuori dall'ambito di applicazione della Convenzione i sistemi di IA utilizzati per la tutela degli interessi relativi alla sicurezza nazionale, per le attività di ricerca volte a testare i sistemi di IA e per le materie relative alla difesa nazionale[60]. Tuttavia, nel caso della sicurezza nazionale, la Convenzione quadro esplicita chiaramente che la tutela degli interessi ad essa legati deve avvenire in coerenza con gli obblighi stabiliti dal diritto internazionale applicabile, e nel rispetto delle istituzioni e dei processi democratici[61]. Tale specificazione non è ripetuta, probabilmente in maniera significativa, nel caso della difesa nazionale[62].

Anche l'*Explanatory Report* della Convenzione quadro sembra mantenere questa distinzione[63], poiché per i sistemi di IA legati agli interessi di sicurezza nazionale elenca un ampio numero di strumenti di diritto internazionale applicabili (tra cui, naturalmente, la CEDU)[64], mentre per le attività relative alla difesa si limita semplicemente a stabilire che la sua esclusione dall'ambito di applicazione della Convenzione non significa che tali attività siano escluse dall'ambito di applicazione del diritto internazionale[65].

[58] Per esempio, la versione della definizione di IA nel precedente documento OECD del 2019 definiva come sistemi IA solo quelli che potevano fornire un output soltanto sulla base di una serie di obiettivi stabiliti da esseri umani ("*for a given set of human-defined objectives*") dunque tenendo al di fuori di essa, per esempio, i sistemi di IA generati da altri sistemi IA.

[59] Art. 3, par. 1, lettere a) e b), Convenzione quadro.

[60] *Ibidem,* art. 3, parr. 2, 3, e 4.

[61] *Ibidem*, art. 3, par. 2.

[62] *Ibidem,* art. 3, par. 4.

[63] *Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* in *Council of Europe Treaty Series*, n. [225] www.coe.int/en/web/artificial-intelligence/cai.

[64] *Explanatory Report*, par. 32.

[65] *Ibidem,* par. 36.

3.2. *Gli obblighi generali ed i principi applicabili all'IA*

La Convenzione quadro stabilisce due obblighi generali: la tutela dei diritti dell'uomo e l'integrità del processo democratico e la protezione dello Stato di diritto.

Riguardo il primo aspetto, viene inserito l'obbligo per le Parti della Convenzione di assicurare che tutte le attività che fanno parte del ciclo di vita dell'intelligenza artificiale siamo conformi agli obblighi di tutela dei diritti fondamentali, sia a livello internazionale che a livello interno[66]. L'assolvimento di tali obblighi viene definito, nell'*Explanatory Report*, come un'obbligazione di risultato[67]. Le spiegazioni, infatti, elencano puntualmente gli strumenti di diritto internazionale da rispettare, includendo anche quelli dell'Unione europea (tra cui la Carta dei diritti fondamentali)[68].

Riguardo invece l'integrità del processo democratico e il rispetto dello Stato di diritto, la Convenzione quadro stabilisce che l'intelligenza artificiale non possa essere utilizzata per mettere a repentaglio l'integrità, l'indipendenza e l'efficacia dei processi democratici e il principio della separazione dei poteri[69].

Nel secondo paragrafo, invece, l'art. 5 continua stabilendo un simile principio per il ciclo di vita dell'intelligenza artificiale, prevedendo la possibilità di avere uguale accesso e partecipazione al dibattito pubblico e nella formazione libera delle loro opinioni[70].

L'*Explanatory Report*, anche in questo caso, fornisce molti dettagli sui comportamenti che le parti contraenti dovranno tenere, elencando una serie di rischi tipici posti dall'intelligenza artificiale, tra cui quelli che riguardano il principio di separazione dei poteri[71].

Riguardo invece i principi applicabili al ciclo di vita dell'intelligenza artificiale, la Convenzione quadro riprende alcuni di quelli che caratterizzano i diritti fondamentali negli ordinamenti nazionali e sovranazionali, come dignità umana, trasparenza, responsabilità, uguaglianza e affidabilità[72]. Vi è tuttavia un principio innovativo, che deriva dall'applicazione del principio di precau-

[66] Convenzione quadro, art. 4.
[67] *Explanatory Report*, cit. par. 38.
[68] *Ibidem,* par. 39.
[69] Convenzione quadro, art. 5, par. 1.
[70] Convenzione quadro, art. 5, par. 2.
[71] *Explanatory Report*, cit. par. 46.
[72] Convenzione quadro, artt. 7-12.

zione all'ambito dell'innovazione tecnologica[73]: il principio dell'innovazione sicura[74]. Tale principio viene definito, nelle spiegazioni alla Convenzione quadro, come un metodo per permettere lo sviluppo di un'innovazione responsabile attraverso l'utilizzo di ambienti controllati (come, per esempio, le c.d. *sandboxes*)[75] che permettano di valutare i rischi posti dall'intelligenza artificiale prima della sua commercializzazione o apertura al pubblico[76].

3.3. *Il meccanismo di gestione del rischio*

In maniera non dissimile da quanto previsto, per esempio, dal regolamento sull'intelligenza artificiale, anche la Convenzione quadro prevede l'obbligo per le parti contraenti di valutare il rischio rappresentato dai sistemi di IA nel corso del loro ciclo di vita[77]. Tale rischio, tuttavia, a differenza di quanto avviene nell'ambito del diritto dell'Unione europea (dove la gestione del rischio è attuata in via generale ma poi è ulteriormente specificata con la valutazione d'impatto sui diritti fondamentali), si concentra soprattutto sui rischi che l'IA pone per la democrazia, lo Stato di diritto ed i diritti umani[78]. Tale gestione del rischio deve avvenire tenendo conto degli obblighi di carattere generale e dei principi sopra esposti, con particolare riferimento al principio di trasparenza e di responsabilità[79]. È dunque ragionevole pensare che la gestione del rischio e la valutazione dell'impatto dell'IA su democrazia, Stato di diritto e diritti fondamentali dovrà coordinarsi, per gli Stati membri dell'Unione europea, con quella prevista dall'*AI Act*.

Le spiegazioni alla Convenzione infatti prevedono che, malgrado lo sforzo per l'adozione di un approccio comune alla gestione del rischio, spetti alle Parti adattare l'obbligo imposto dalla Convenzione al proprio quadro regolatorio[80].

[73] Il principio di precauzione, nell'ordinamento dell'Unione, è citato all'art. 191 del TFUE, ma con riferimento alla politica ambientale.

[74] Convenzione quadro, art. 13.

[75] Sulle *sandboxes* (anche se con riferimento all'*AI Act*), v. G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle regulatory sandboxes*, in questo *Fascicolo Speciale,* www.aisdue.eu/gabriele-rugani-la-promozione-di-strumenti-di-co-regolazione-dellintelligenza-artificiale-nellai-act-con-particolare-riferimento-alle-regulatory-sandboxes/.

[76] *Explanatory Report*, cit. parr. 90-91.

[77] Convenzione quadro, Titolo V, *Assessment and mitigation of risks and adverse impacts*.

[78] Convenzione quadro, art. 16, par. 1.

[79] *Explanatory Report*, cit. par. 105.

[80] *Ibidem,* par. 106.

La descrizione dei sistemi di gestione del rischio, che avviene di regola all'inizio del ciclo di vita dell'IA, dovrà comunque sempre soppesare la sua gravità e probabilità, assicurare il suo regolare aggiornamento, mettere a disposizione del pubblico la documentazione che dia conto di tali rischi e prevedere l'obbligo di testare i sistemi di IA[81]. Anche nelle spiegazioni si descrive come la gestione del rischio effettuata all'inizio del ciclo di vita dell'intelligenza artificiale sia solo il primo passaggio di un processo più complesso, che tiene anche conto della sostenibilità ambientale e della salute[82], e che deve sempre prevedere la possibilità di aggiornare e rivalutare il rischio[83].

Gli obblighi di trasparenza sono poi, sempre nelle spiegazioni, ulteriormente dettagliati, stabilendo che i soggetti che sviluppano l'IA devono mettere a disposizione la documentazione tecnica che permette di potere valutare il rischio e di doverla aggiornare, oltre che di dovere dare sempre la possibilità a dei soggetti indipendenti di effettuare dei controlli[84].

La Convenzione quadro prevede anche, in linea con la disciplina dell'Unione europea, la possibilità per gli Stati che ne faranno parte di vietare determinate tipologie di intelligenza artificiale che costituiscano, sulla base degli strumenti di gestione del rischio, un pericolo per la democrazia, i diritti fondamentali e lo Stato di diritto[85].

Il sistema di gestione del rischio, governato dai principi applicabili al ciclo di vita dell'IA, sembra dunque ben coordinarsi con gli ulteriori e più generali sistemi di gestione del rischio che potrebbero essere previsti dai legislatori nazionali in applicazione dell'*AI Act*, che sarà esaminata nel paragrafo successivo.

3.4. *Il ruolo dell'Unione europea nella Convenzione quadro*

Meritano da ultimo una menzione le disposizioni della Convenzione quadro che prevedono esplicitamente un ruolo dell'Unione europea nella sua attuazione[86].

[81] Convenzione quadro, art. 16, par. 2.

[82] *Explanatory Report*, cit. par. 108.

[83] *Ibidem,* par. 109.

[84] *Ibidem,* par. 109.

[85] Convenzione quadro, art. 16, par. 4.

[86] Anche alla luce del rinnovato dibattito sull'adesione – non priva di ostacoli – dell'Unione europea alla Convenzione europea dei diritti dell'uomo, su cui v. N. Bergamaschi, *Prime considerazioni sul nuovo tentativo di adesione dell'Unione alla CEDU e sui suoi princi-*

Tale ruolo si declina in due aspetti. Il primo, che prevede che l'applicazione della disciplina dell'Unione applicabile all'IA abbia luogo senza creare pregiudizio alla Convenzione[87]. Il secondo, invece, che prevede espressamente la possibilità che l'Unione europea diventi una Parte contraente della Convenzione[88].

Riguardo al primo aspetto, le spiegazioni precisano che la menzione espressa del diritto dell'Unione serva soprattutto nei rapporti tra gli Stati membri, che potranno dunque avvalersene, per esempio, per denunciare le violazioni del diritto dell'Unione che costituiscano anche una violazione della Convenzione[89]. Si chiarisce poi ulteriormente che la Commissione che ha redatto la Convenzione quadro ritiene che, all'interno della nozione di diritto dell'Unione, ricadano «measures, principles and procedures provided for in the European Union legal order, in particular laws, regulations or administrative provisions as well as other requirements, including court decisions»[90]. Questo è probabilmente il primo caso in cui una Convenzione promossa dal Consiglio d'Europa cita in maniera così diretta il diritto dell'Unione e la giurisprudenza della Corte di giustizia, ed è anche il segno della maggiore e rinnovata attenzione nei confronti dell'autonomia e delle caratteristiche specifiche del diritto dell'Unione europea[91].

All'art. 30, invece, la Convenzione prevede la possibilità che l'Unione europea la possa ratificare, diventando dunque parte dell'ordinamento dell'Unione[92]. Rimane tuttavia da verificare se tale Convenzione possa configurarsi come un accordo internazionale concluso esclusivamente dall'Unione oppure come accordo misto, concluso sia dall'Unione che dagli Stati membri[93]. Una risposta a questa domanda sembra essere stata data dalla firma, da parte della Commissione europea, della Convenzione del Consiglio d'Europa all'atto della sua apertura il 5 settembre 2024[94]. Tale firma

pali ostacoli, in *Quaderni AISDUE*, 2024, www.aisdue.eu/nicola-bergamaschi-prime-considerazioni-sul-nuovo-tentativo-di-adesione-dellunione-alla-cedu-e-sui-suoi-principali-ostacoli/.

[87] Convenzione quadro, art. 27, par. 2.

[88] Convenzione quadro, art. 30, par. 1.

[89] *Explanatory Report*, cit. par. 147.

[90] *Ibidem.*

[91] Questo anche alla luce dell'eventuale parere che la Corte di giustizia potrebbe dovere rendere sulla compatibilità della Convenzione con i Trattati.

[92] V. per esempio, Corte giust. 30 aprile 1974, 181/73, *Haegeman*, punti 3-5.

[93] Sulla differenza tra accordi conclusi esclusivamente dall'UE e accordi misti si veda M. Gatti, P. Manzini, *External Representation of the European Union in the Conclusion of International Agreements*, in *CMLR*, 2012, p. 1703 ss.

[94] *Commission signed the Council of Europe Framework Convention on Artificial Intel-*

esprime la volontà dell'Unione e degli Stati membri di vincolarsi al rispetto della Convenzione. La sua eventuale conclusione da parte dell'Unione la renderebbe comunque parte dell'a*cquis* dell'Unione e potrebbe provocarne persino l'applicazione davanti ai giudici degli Stati membri[95].

La procedura da seguire per ratificare la Convenzione è dettata dall'art. 218 TFUE, che prevede che la Commissione formuli una proposta di decisione al Consiglio, l'approvazione da parte del Parlamento europeo, e la possibilità che gli Stati, il Parlamento, il Consiglio o la Commissione richiedano alla Corte di giustizia un parere sulla compatibilità dell'accordo con i Trattati.

È interessante notare come, in questo caso, non sembrino trovare applicazione le disposizioni dell'art. 218 TFUE che rafforzano la procedura di conclusione degli accordi internazionali nel caso in cui si tratti di aderire alla CEDU[96]. La CEDU è infatti menzionata espressamente, cosa che non avviene invece riguardo la possibilità di entrare a fare parte di altre Convenzioni previste dal Consiglio d'Europa.

Qualora dunque l'Unione decida di stipulare la Convenzione quadro sull'intelligenza artificiale, la procedura per la sua conclusione potrebbe paradossalmente terminare prima di quella per l'adesione alla CEDU.

ligence and human rights, democracy and the rule of law, 5 September 2024, digital-strategy.ec.europa.eu/en/news/commission-signed-council-europe-framework-convention-artificial-intelligence-and-human-rights.

[95] Sull'effetto diretto degli accordi internazionali conclusi dall'Unione, si vedano F. Martines, *Direct Effect of International Agreements of the European Union,* in *European Journal of International Law,* 2014, p. 129 ss. e Á. Mohay *The status of international agreements concluded by the European Union in the EU legal order*, in *Pravni vjesnik*, 2017, p. 151 ss.

[96] Come, per esempio, il voto all'unanimità da parte del Consiglio, previsto all'art. 218, par. 8, secondo comma TFUE.

4. *Il regolamento sull'intelligenza artificiale e le questioni aperte sulla gestione del rischio ed il principio democratico*

Il regolamento sull'intelligenza artificiale (*AI Act*) è stato estesamente commentato sia su questa Rivista[97] che altrove[98] ben prima della sua recente adozione da parte del Parlamento europeo e del Consiglio[99]. In questa sede, dunque, non mi concentrerò sugli aspetti di carattere generale e sistemico, e neppure sulle questioni più particolari (benché di estremo interesse, quali quelle sulle norme armonizzati)[100] del regolamento e mi limiterò a formulare alcune osservazioni sulla rilevanza che potrebbero avere gli strumenti di gestione del rischio messi a disposizione dal regolamento nel fornire possibilità di tutela nei confronti delle minacce alla democrazia e allo Stato di diritto.

Tali strumenti sono, essenzialmente, la gestione del rischio di carattere generale per le IA ad alto rischio e quella, più specifica, di valutazione dell'impatto sui diritti fondamentali e su democrazia e Stato di diritto.

[97] Si vedano i contributi di E. Cirone, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali* in questo *Fascicolo Speciale*, www.aisdue.eu/enza-cirone-lai-act-e-lobiettivo-mancato-di-promuovere-uno-standard-globale-per-la-tutela-dei-diritti-fondamentali/. F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea* in questo *Fascicolo Speciale*, www.aisdue.eu/federico-ferri-il-giorno-dopo-la-rivoluzione-prospettive-di-attuazione-del-regolamento-sullintelligenza-artificiale-e-poteri-della-commissione-europea/. M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?* in questo *Fascicolo Speciale,* www.aisdue.eu/marco-inglese-il-regolamento-sullintelligenza-artificiale-come-atto-per-il-completamento-e-il-buon-funzionamento-del-mercato-interno/. S. Villani, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?* in questo *Fascicolo Speciale*, www.aisdue.eu/susanna-villani-il-sistema-di-vigilanza-sullapplicazione-dellai-act-ognun-per-se/.

[98] V. per esempio C. Novelli, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione* in *federalismi.it*, 2024, p. 95 ss. C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, L. Floridi, *Taking AI risks seriously: a new assessment model for the AI Act*, in *AI & Society*, 2023, p. 1 ss. J. Schuett, *Risk management in the artificial intelligence act* in *European Journal of Risk Regulation*, 2023, p. 1 ss. M. Almada, N. Petit, *The EU AI act: a medley of product safety and fundamental rights?* in *Robert Schuman Centre Working Paper*, 2023, cadmus.eui.eu/handle/1814/75982.

[99] Il regolamento è stato adottato dal Parlamento europeo e dal Consiglio il 13 giugno 2024 ed è stato pubblicato in Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024.

[100] Su cui v. A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale,* in questo *Fascicolo Speciale*, www.aisdue.eu/annalisa-volpato-il-ruolo-delle-norme-armonizzate-nellattuazione-del-regolamento-sullintelligenza-artificiale/.

4.1. *I riferimenti al principio democratico ed ai diritti fondamentali nella parte introduttiva del regolamento*

Prima di menzionare tali strumenti, è però necessario offrire una panoramica dei diversi riferimenti al principio democratico ed ai diritti fondamentali, soprattutto nella parte introduttiva del regolamento[101]. Questi riferimenti, infatti, ci danno la misura di come, nei lavori sul testo dell'*AI Act*, il baricentro dell'atto legislativo si sia spostato dalla logica della sicurezza dei prodotti con l'obiettivo di armonizzare il mercato unico digitale (logica che caratterizza comunque in maniera netta il regolamento)[102] ad una maggiore preoccupazione per il rispetto dei diritti fondamentali. Tale preoccupazione riflette dunque l'emersione di un quadro giuridico europeo, tra cui in questo momento sembra potere assumere una certa importanza la Convenzione quadro del Consiglio d'Europa, che ha come obiettivo principale proprio quello di tutelare la democrazia nello sviluppo dell'innovazione tecnologica.

La necessità di proteggere i diritti fondamentali, tra cui vengono espressamente menzionati la democrazia e lo Stato di diritto, emergono fin dal primo considerando del regolamento[103]. Nel secondo, invece, viene ribadita l'importanza di un'intelligenza artificiale che rispetti i valori dell'Unione, ed in particolare lo Stato di diritto e la democrazia[104]. Anche al considerando

[101] Tali riferimenti si fondano su un quadro generale di tutela dei diritti fondamentali dell'Unione che si sta adattando alle innovazioni tecnologice. Sul punto v. A. Adinolfi, *Evoluzione tecnologica e diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, n. 15, 2023, p. 323 ss., www.aisdue.eu/adelina-adinolfi-evoluzione-tecnologica-e-tutela-dei-diritti-fondamentali-qualche-considerazione-sulle-attuali-strategie-normative-dellunione/, nonché A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: brevi considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), I*ntelligenza artificiale e diritto: una rivoluzione? – Volume 1: Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, p. 127 ss. P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?* in *DUE – Osservatorio europeo*, 2022, images.dirittounioneeuropea.eu/f/sentenze/documento_29xPa_DUE.pdf.

[102] Su questo v. in particolare M. Inglese, *op. cit*., p. 6 ss.

[103] *AI Act*, considerando 1: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione […] garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("Carta"), compresi la democrazia, lo Stato di diritto […]».

[104] *AI Act*, considerando 2: «Il presente regolamento dovrebbe essere applicato con-

n. 8 viene, di nuovo, ripetuta l'importanza dei diritti fondamentali, e tra di essi vengono espressamente menzionati lo Stato di diritto e la democrazia, questa volta però come interessi pubblici alla cui protezione deve tendere il quadro giuridico dell'Unione sull'IA[105]. L'esigenza di rispettare i diritti fondamentali e di permettere il controllo democratico viene poi invocata nell'ambito dell'alfabetizzazione in materia di IA, passaggio che è ritenuto dalle istituzioni molto importante per diffondere la conoscenza in materia di intelligenza artificiale[106]. La democrazia e lo Stato di diritto, poi, vengono di nuovo menzionati nel considerando dedicato alle tecniche di manipolazione, sfruttamento e controllo sociale realizzate tramite IA, che sono tra le IA proibite[107], e al considerando 61 e 62, con riferimento ai sistemi IA ad alto rischio coinvolti nei processi democratici e nell'amministrazione della giustizia. L'importanza del principio democratico viene evidenziata anche con riguardo ai rischi sistemici posti dalle IA generaliste per il processo democratico, attraverso, per esempio, il rischio di disinformazione[108].

Merita invece forse ancora maggiore attenzione il riferimento diretto, fatto al considerando 120, agli obblighi stabiliti dal *Digital Services Act* per le piattaforme online e i motori di ricerca online di grandi dimensioni di individuare i rischi posti dalla diffusione di contenuti ingannevoli o manipolati nei confronti, per esempio, del processo democratico. Tale precisazione, infatti, riflette l'emersione di una disciplina orizzontale destinata a disciplinare le innovazioni tecnologiche ed i rischi per il principio democratico ed i diritti fondamentali.

La necessità di proteggere i diritti fondamentali, tra cui principio democratico e Stato di diritto, viene di nuovo poi ribadita al considerando 176, dove le istituzioni sembrano volere chiudere il cerchio della parte introdut-

formemente ai valori dell'Unione sanciti dalla Carta agevolando la protezione delle persone fisiche, delle imprese, della democrazia e dello Stato di diritto […]».

[105] *AI Act*, considerando 8: «Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo […] la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto […]».

[106] *AI Act*, considerando 20: «Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA […]». Anche al considerando 56 viene menzionata l'esigenza dell'alfabetizzazione in materia di IA.

[107] *AI Act,* considerando 28.

[108] *AI Act,* considerando 110.

tiva del regolamento ribadendo la conformità del regolamento e degli atti di esecuzione ad esso collegati con il principio di sussidiarietà e proporzionalità[109].

Nel testo del regolamento, invece, il riferimento al principio democratico emerge sin dall'art. 1, in cui si delimita l'oggetto. Tale oggetto promuove la costituzione di un'IA antropocentrica ed affidabile, che può essere garantita soltanto da un elevato livello di tutela dei diritti fondamentali (tra cui vengono di elencati la democrazia e lo Stato di diritto).[110] Altri riferimenti si possono trovare all'art. 74, par. 8, per i sistemi di IA ad alto rischio legati ai processi democratici, ed al par. 8 dell'Allegano III, sui sistemi di IA ad alto rischio.

Il riferimento alla tutela del principio democratico ed ai diritti fondamentali (incluso il rispetto dello Stato di diritto) sembra avere lo scopo di ricordare al giudice nazionale, che sarà impegnato nell'interpretazione ed applicazione del regolamento, che questo strumento giudico deve essere interpretato in conformità con i diritti fondamentali così come descritti nella Carta dei diritti fondamentali e nella giurisprudenza della Corte di giustizia.

4.2 *La gestione del rischio e la valutazione di impatto in materia di diritti fondamentali*

Dopo i riferimenti al principio democratico nella parte introduttiva del regolamento, è necessario menzionare il sistema di gestione del rischio per le IA ad alto rischio e di valutazione d'impatto in materia di diritti fondamentali, cui si accompagna il potere di richiesta di informazioni per le autorità responsabili in materia di diritti fondamentali di cui all'art. 77. Tale sistema,

[109] *AI Act,* considerando 176: «Poiché l'obiettivo del presente regolamento, vale a dire migliorare il funzionamento del mercato interno e promuovere la diffusione di un'IA antropocentrica e affidabile, garantendo nel contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e promuovendo l'innovazione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata o degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'art. 5 TUE. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso art.».

[110] *AI Act*, art. 1, par. 1: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione».

che nel caso in cui l'Unione aderisca, dovrà coordinarsi con quello previsto dalla Convenzione quadro del Consiglio d'Europa, costituisce la principale innovazione normativa proposta dal regolamento.

L'obbligo di attivare tale sistema è applicabile soltanto alle IA ad alto rischio[111]. Il sistema è definito dal regolamento come «un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici»[112].

La caratteristica principale di questo sistema (e forse anche la sua maggiore onerosità) che, come si vedrà più oltre, è composto di quattro sezioni, è dunque quella di richiedere un aggiornamento costante e sistematico. Questo elemento, infatti, implica la sua revisione ed aggiornamento a cadenza regolare, onerando significativamente gli sviluppatori di tali sistemi e rendendone più difficile la commercializzazione. Dal punto di vista, però, dei potenziali rischi per il principio democratico ed i diritti fondamentali, tuttavia, questa caratteristica del sistema di gestione del rischio si traduce in una maggiore tutela per i soggetti deboli e per i consumatori.

Le fasi di cui è composto il sistema di gestione del rischio sono quattro: a) identificazione e analisi dei rischi per la salute, la sicurezza ed i diritti fondamentali; b) stima e valutazione dei rischi che possono emergere da un uso improprio dell'IA; c) valutazione e stima dei rischi successivi all'immissione sul mercato; d) adozione di misure di gestione dei rischi opportune e mirate a limitare i rischi individuati al punto a)[113].

Leggendo poi l'art. 9, par. 2, dell'*AI Act* in combinato disposto con altre sue parti, tra cui, per esempio, il considerando 1, il riferimento ai diritti fondamentali è da intendersi necessariamente a quelli inclusi nella Carta, e tra di essi hanno un'importanza particolare la democrazia e lo Stato di diritto (oltre alla protezione dell'ambiente, che però esorbita l'obiettivo di questo scritto)[114].

[111] Tali sistemi sono indicati all'art. 6, par. 1, e all'allegato III dell'AI act. Tra di essi, per esempio, vi sono quelli per la gestione dell'immigrazione, delle procedure di asilo e di controllo alle frontiere e quelli relativi all'amministrazione della giustizia e al processo democratico. Un Autore ha tuttavia sostenuto che sia opportuno che anche le IA a rischio basso o minimo seguano volontariamente lo stesso schema: v. J. Schuett, *op. cit.,* p. 7.

[112] *AI Act*, art. 9, par. 2. Su tale sistema, e sulle differenze e gradazioni nei diversi atti legislativi dell'Unione che lo applicano, v. G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age* in *CMLR,* 2022, p. 473 ss.

[113] Per un'analisi dettagliata delle quattro fasi, v. J. Schuett, *op. cit.,* pp. 9-13.

[114] *AI Act*, considerando 1: «[…] garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti

Dunque, le persone fisiche o giuridiche che intendono commercializzare un sistema di IA, secondo il regolamento, devono considerare i rischi per la democrazia e, più generalmente, per i diritti fondamentali. Rimane però ancora da capire come tale valutazione e gestione del rischio possa essere fatto in concreto, e quali indicazioni daranno i soggetti che la Commissione dovrà indicare come responsabili ai sensi del regolamento[115].

Riguardo invece il sistema di gestione del rischio, nonostante la proposta della Commissione prevedesse sin dall'inizio il meccanismo di cui all'art. 9, par. 2, che includeva anche, tra i criteri di valutazione, il rispetto dei diritti fondamentali, non vi era, in tale proposta, la previsione di uno strumento di valutazione dell'impatto limitato ai soli diritti fondamentali. Tale strumento è stato inserito su proposta del Parlamento[116] nel corso dei negoziati che hanno preceduto l'adozione del testo finale, ed è ora previsto all'art. 27 del regolamento[117].

A prima vista, l'art. 27 esplicita un obbligo che era già insito nella prima formulazione dell'art. 9, dove si dice (come è stato esposto nel paragrafo precedente), che il sistema di gestione del rischio deve tenere conto dei rischi per i diritti fondamentali. Si aggiunge, tuttavia, uno strumento più circostanziato, che si integra nel più generale sistema di gestione del rischio e che, verosimilmente, potrebbe essere gestito principalmente da soggetti privati[118].

Tale strumento, tuttavia, è maggiormente limitato rispetto a quello generale sia dal punto di vista dell'ambito di applicazione personale che da quello dell'ambito di applicazione materiale.

fondamentali dell'Unione europea ("Carta"), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente […]».

[115] Si rimanda qui alle osservazioni fatte da E. Cirone, *op. cit.,* p. 12-13.

[116] *Ibidem,* p. 14.

[117] La valutazione di impatto sui diritti fondamentali viene introdotta per la prima volta nella lista di emendamenti pubblicata dal Parlamento europeo alla posizione del Consiglio in prima lettura. Questo testo ha fatto poi da base ai triloghi che si sono succeduti nel corso della fine del 2023 e dell'inizio del 2024, che hanno portato all'adozione del testo definitivo. V. art. 29, emendamento n. 413, *Emendamenti del Parlamento europeo, approvati il 14 giugno 2023, alla 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*.

[118] V. di nuovo quanto sostenuto e la letteratura citata da E. Cirone, *op. cit.,* p. 16, dove si discute il processo di 'privatizzazione' della verifica della compatibilità con gli standard in materia di rispetto dei diritti fondamentali. Si potrebbe aggiungere che questo avviene anche in altri ambiti, come, per esempio, negli studi sulla compatibilità della legislazione nazionale con il quadro dell'Unione.

L'ambito di applicazione personale, infatti, è limitato ai soli *deployer*[119]. Dunque, solo i soggetti che utilizzano un sistema IA sotto la propria autorità sono tenuti ad effettuare tale valutazione del rischio, e, tra di essi, soltanto quelli che sono organismi di diritto pubblico, oppure sono enti privati che forniscono servizi pubblici o quelli di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c)[120].

L'ambito di applicazione materiale, invece, è ristretto alle IA ad alto rischio, ad esclusione di quelle destinate a essere usati nel settore elencati nell'allegato III, punto 2[121].

La valutazione di impatto si compone, ai sensi delle lettere da a) ad f) del primo paragrafo dell'art. 27, di sei parti: a) la descrizione dei processi in cui il sistema sarà utilizzato, b) una descrizione del tempo e della frequenza di utilizzo, c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico, d) i rischi specifici per le categorie interessate, e) la descrizione dell'attuazione delle misure di sorveglianza umana, ed f) le misure da adottare per mitigare eventuali rischi che si presentino.

Rimangono alcune questioni aperte: prima di tutto, in che rapporto sta questa valutazione di impatto con quella prevista nel più generale sistema di gestione del rischio. Il par. 2 dell'art. 27 sembra suggerire che si tratti di due valutazioni diverse, ma che il *deployer* possa utilizzare, per esempio, la valutazione d'impatto già effettuata dal fornitore in prima istanza, e che la valutazione d'impatto già effettuata ai sensi di altre disposizioni di diritto derivato possa integrarsi con quella prevista all'art. 27[122]. È poi compito del *deployer* notificare l'esito della valutazione all'autorità responsabile per la sorveglianza del mercato[123].

Il par. 5 dell'art. 27, tuttavia, assegna all'Ufficio IA la competenza a redigere un questionario semplificato per permettere ai *deployer* di assolve-

[119] I *deployer* vengono definiti all'art. 3, comma 1, numero 4 dell'AI act come: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

[120] Questi ultimi sono i sistemi di IA utilizzati per valutare l'affidabilità creditizia o il merito di credito delle persone fisiche (ad eccezione di quelli utilizzati per il contrasto alle frodi finanziarie) e quelli utilizzati per la valutazione dei rischi e la determinazione dei prezzi delle assicurazioni sulla vita e assicurazioni sanitarie.

[121] E cioè: «Infrastrutture critiche: i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità».

[122] *AI Act*, art. 27, par. 4.

[123] *AI Act*, art. 27, par. 3.

re all'obbligo. Potrebbe essere opportuno, in questo caso, coinvolgere l'Agenzia per i Diritti Fondamentali dell'Unione europea nell'elaborazione del questionario.

Rimangono ora da analizzare i poteri delle autorità che tutelano i diritti fondamentali, aspetto dell'atto che potrebbe passare a prima vista inosservato. Ai sensi dell'art. 77 dell'*AI Act*, le autorità che tutelano i diritti fondamentali a livello nazionale ed europeo, «hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione»[124].

Oltretutto, qualora la documentazione prodotta non sia sufficiente per accertare un'eventuale violazione, le autorità nazionali hanno il potere di richiedere all'autorità di vigilanza del mercato di effettuare una prova del sistema IA per capire, in concreto, quali problematiche potrebbe sollevare[125].

Tali autorità dovranno essere designate entro i tre mesi successivi all'entrata in vigore del regolamento dagli Stati membri e comunicate alla Commissione[126].

Questi poteri, che potranno essere giudicati compiutamente soltanto dopo la decorrenza della data per l'applicazione dell'*AI Act*[127], sembrano piuttosto ampi, e potranno certamente restituire centralità alle autorità che hanno mandato, a livello nazionale ed europeo, nei confronti della tutela dei diritti fondamentali nell'Unione europea.

Il quadro che emerge dall'*AI Act*, dunque, sembra disegnare una complessa impalcatura finalizzata alla gestione del rischio ed alla valutazione dell'impatto in materia di diritti fondamentali, tra cui anche la democrazia, di cui ci si occupa in particolare in questo saggio. Il rischio che questa impalcatura, una volta che la Commissione e le autorità di vigilanza avranno dato attuazione alle parti dell'*AI Act* che necessitano di atti di diritto derivato, implichi la "burocratizzazione" del meccanismo di valutazione del rischio è certamente elevato. Con esso, sembra profilarsi anche l'eventualità che il meccanismo di gestione e valutazione del rischio venga automatizzato attraverso il ricorso a soggetti privati che certamente, nei prossimi anni, si organizzeranno per fornire questo tipo di servizi ai soggetti pubblici e privati che dovranno conformarsi agli obblighi previsti dal regolamento.

[124] *AI Act*, art. 77, par. 1.

[125] *AI Act*, art. 77, par. 3.

[126] *AI Act*, art. 77, par. 2.

[127] Due anni dopo la sua entrata in vigore, secondo l'art. 113, par. 2.

Dunque, se da un lato gli obblighi per i soggetti coinvolti sono certamente consistenti, dall'altro, l'ordinamento dell'Unione sembra caratterizzato dalla certezza e dalla prevedibilità degli oneri.

5. *Il* Media Freedom Act*, il* Digital Services Act *ed i profili applicabili alla tutela del principio democratico*

Vi sono altri strumenti di diritto derivato dell'Unione che possono rivelarsi utili ai fini di assicurare un livello adeguato di protezione per la democrazia ed i diritti fondamentali. Tra di essi sono da menzionare alcuni profili del *Media Freedom Act* e del *Digital Services Act.*

5.1. *Il* Media Freedom Act

Il *Media Freedom Act*[128]*,* che è entrato in vigore recentemente, è parte di un complesso sistema di misure sia legislative che non legislative introdotte dalla Commissione europea per tutelare l'indipendenza dei mezzi di comunicazione[129].

La rilevanza di questo regolamento appare evidente sin dal secondo considerando, dove i co-legislatori hanno precisato che la tutela della libertà e del pluralismo dei media sono elementi fondamentali per la democrazia e lo Stato di diritto[130].

Gli strumenti che questo regolamento mette a disposizione per tutelare i media come "pilastri" della democrazia sono almeno tre: le disposizioni a tutela dell'indipendenza dei media[131], l'istituzione di un comitato europeo per i servizi dei media[132], e gli obblighi per le piattaforme online di dimensioni molto grandi[133].

L'art. 5 del regolamento istituisce l'obbligo che gli Stati membri metta-

[128] Regolamento (UE) 2024/1083.

[129] Ad esempio, la direttiva (UE) 2024/1069 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, sulla protezione delle persone attive nella partecipazione pubblica da domande manifestamente infondate o procedimenti giudiziari abusivi.

[130] *Media Freedom Act,* considerando 2: «Considerato il ruolo unico dei servizi di media, tutelare la libertà e il pluralismo dei media quali due dei pilastri principali della democrazia e dello Stato di diritto costituisce un aspetto essenziale per il buon funzionamento del mercato interno dei servizi di media».

[131] *Media Freedom Act*, art. 5.

[132] *Media Freedom Act*, art. 8.

[133] *Media Freedom Act*, art. 18.

no i mezzi di informazione nelle condizioni di essere indipendenti dagli altri poteri che caratterizzano l'ordinamento giuridico. Oltre a questo, al par. 2, l'art. 5 stabilisce che gli Stati membri debbano nominare i membri dei consigli di amministrazione di eventuali mezzi di comunicazione pubblici in maniera tale da preservarne l'indipendenza. Prevede oltretutto che il direttore e i membri del consiglio di amministrazione debbano essere nominati in seguito a procedure imparziali e trasparenti e che non possano essere rimossi se non in via eccezionale, e dunque non per riflettere, per esempio, il nuovo equilibrio politico venutosi a creare per effetto di una tornata elettorale particolarmente favorevole ad un partito che precedentemente era in minoranza.

L'istituzione di un comitato per i servizi media ha invece il fine di creare una vera e propria autorità di vigilanza europea, che sostituisce il precedente gruppo dei regolatori europei per i servizi di media audiovisivi (ERGA)[134].

Tale comitato, che è composto da rappresentanti delle autorità nazionali di regolamentazione, prende le sue decisioni a maggioranza di due terzi ed è indipendente dal potere politico ed istituzionale sia nazionale che dell'Unione[135].

Tra le funzioni principali del comitato, è sicuramente molto importante quella di proporre, di propria iniziativa o su richiesta della Commissione, pareri sia sulle «misure normative o amministrative che possono incidere in modo significativo sul funzionamento dei fornitori di servizi di media nel mercato interno dei servizi di media»[136] che «in merito alle concentrazioni del mercato dei media che possono incidere sul funzionamento del mercato interno dei servizi di media»[137].

All'interno delle funzioni del comitato ricadono poi gli obblighi nei confronti delle piattaforme online di dimensioni molto grandi di assicurare che i mezzi di comunicazione abbiano a disposizione gli strumenti necessari per qualificarsi come "fornitori di servizi dei media" e dunque per distinguersi da altri soggetti che diffondono informazioni a titolo personale, per rendere più difficile, per esempio, la diffusione di notizie false[138].

Questo regolamento, dunque, istituisce un meccanismo di controllo, da attuarsi tramite il comitato, che permette l'applicazione di un livello uniforme di protezione dell'indipendenza dei mezzi di comunicazione, sia a mezzo stampa che elettronici, nel territorio dell'Unione europea.

Anche in questo caso, con la riserva e l'evidente necessità di vedere nella pratica l'applicazione di queste innovazioni, sembra che, attraverso il diritto

[134] *Media Freedom Act*, art. 8, par. 2.

[135] *Media Freedom Act*, art. 9.

[136] *Media Freedom Act*, art. 13, par. 1, lettera f).

[137] *Media Freedom Act,* art. 13, par. 1, lettera h).

[138] *Media Freedom Act,* art. 17.

dell'Unione, si siano introdotti strumenti che rendono più complicato per i partiti e per la politica nazionale ed europea utilizzare strumentalmente i mezzi di comunicazione, e che permettano dunque di tutelare in maniera più efficiente l'ordinamento democratico.

5.2. *Il* Digital Services Act

Il regolamento sul mercato unico dei servizi digitali (*Digital Services Act*) è lo strumento con cui l'Unione europea disciplina le piattaforme ed i motori di ricerca che operano nel mercato unico digitale[139]. Il *Digital Services Act,* come l'*AI Act* e la Convenzione quadro del Consiglio d'Europa, è caratterizzato da un sistema di valutazione del rischio "sistemico" nei confronti delle piattaforme e dei motori di ricerca molto grandi, che include al suo interno l'esigenza di valutare i rischi nei confronti dei diritti fondamentali[140]. Tuttavia, a differenza degli strumenti che abbiamo visto più sopra, tale meccanismo sembra concentrarsi maggiormente sui diritti fondamentali che qualificano i cittadini dell'Unione come consumatori, anziché come soggetti politici. Questo spiega, probabilmente, come mai possono ritrovarsi riferimenti a questo regolamento sia nell'*AI Act* che nel *Media Freedom Act.*

La valutazione del rischio sistemico deve essere fatta entro quattro mesi dalla designazione, da parte della Commissione, della piattaforma o del motore di ricerca come "molto grandi"[141]. In questo caso, dunque, il possibile rischio sistemico per la democrazia non viene menzionato direttamente[142].

Alla luce della lettura degli obblighi previsti a tutela dei diritti fondamentali e del principio democratico sia nel testo dell'*AI Act* che del *Media Freedom Act*, tuttavia, la valutazione del rischio sistemico prevista dal *Digital Services Act* sembra assumere un'importanza ancora maggiore. Sembra difficile, dunque, che i meccanismi di gestione e valutazione del rischio previsti dagli atti legislativi più recenti, ma anche nei primi regolamenti che hanno disciplinato l'intelligenza artificiale, possano rimanere separati.

[139] Regolamento (UE) 2022/2065.

[140] *Digital Services Act*, art. 34, par. 1, lettera b).

[141] *Digital Services Act,* art. 33, par. 6.

[142] Si veda, per esempio, la seguente ricerca che studia un possibile meccanismo per la valutazione di un rischio sistemico per la democrazia proveniente da piattaforme online: M. Loi, *Making sense of the Digital Services Act How to define platforms' systemic risks to democracy* in *Algoritmic Watch*, 2023, algorithmwatch.org/de/wp-content/uploads/2023/08/AlgorithmWatch_Risk_Assessment-DSA.pdf.

6. *Conclusione*

Giungendo al termine di questo saggio, il lettore potrà apprezzare la complessità e, per certi versi, anche la raffinatezza del sistema congegnato dal Consiglio d'Europa e dall'Unione europea per proteggere i cittadini degli Stati membri, e gli Stati stessi, dai rischi nei confronti del principio democratico e dei diritti fondamentali.

Proprio per questo, riprendendo il titolo significativo di uno degli scritti del Fascicolo in cui è ospitato questo contributo, siamo davvero ancora soltanto all'inizio del "giorno dopo la rivoluzione"[143]. Le dimensioni e le conseguenze di un intervento normativo così vasto e stratificato non permettono dunque una risposta definitiva, ma lasciano spazio ad almeno tre domande.

Primo, alla luce dell'analisi qui condotta sembra allargarsi il divario tra lo spazio in cui è applicabile uno standard elevato di tutela previsto dalla disciplina (internazionale e sovranazionale) europea e tutto quello che c'è al di fuori (tra cui, a titolo meramente esemplificativo, Cina, Stati Uniti, Regno Unito, India). Le Nazioni Unite, dopo la risoluzione illustrata all'inizio di questo saggio, saranno capaci di proporre una soluzione di compromesso (una convenzione) che spinga gli Stati che hanno uno standard di tutela dei diritti inferiore a ridurre questo divario (che potrebbe certamente causare problemi di competitività all'industria digitale europea), oppure continuerà ad allargarsi? E l'Unione saprà adeguare, se si rivelerà necessario, il suo quadro normativo per favorire un migliore bilanciamento tra la protezione dei diritti e la promozione dell'innovazione?

Secondo, l'interazione tra i meccanismi di valutazione del rischio previsti a livello internazionale (come quello del Consiglio d'Europa) e sovranazionale (per esempio, nell'*AI Act* e nel *Digital Services Act*) è complessa già da sola, e lo è ancora di più nel quadro dei complicati rapporti che riguardano l'adesione dell'Unione alla CEDU. È possibile dunque assicurare una tutela efficace e completa al principio democratico anche nell'ipotesi in cui l'Unione non riesca a completare l'adesione alla CEDU? Questo, oltretutto, alla luce del fatto che l'Unione potrebbe diventare parte della Convenzione del Consiglio d'Europa in materia di intelligenza artificiale, pur non essendo parte (o comunque ben prima di divenire parte) della CEDU.

Terzo, come possono coordinarsi tra di loro i meccanismi di gestione e

[143] F. Ferri, *op. cit.,* p. 2.

valutazione del rischio previsti dai diversi strumenti di diritto derivato ed i complessi obblighi di controllo che il diritto dell'Unione attribuisce alle autorità nazionali ed alla stessa Commissione?

Il giorno dopo la rivoluzione, dunque, se è lecito pensare con ottimismo alla varietà degli strumenti giuridici a disposizione, non si può dimenticare che ora spetta ai governi (nazionali e dell'Unione) ed alla politica (di nuovo, nazionale e dell'Unione) decidere a quali condizioni avvalersene.

Abstract (ita)

Diverse organizzazioni internazionali, tra cui il Consiglio d'Europa, si stanno affrettando nel costruire un quadro giuridico convenzionale che permetta lo sviluppo e la commercializzazione di intelligenze artificiali che non entrino in conflitto con il principio democratico ed i diritti fondamentali. Anche l'Unione europea, con l'*AI Act* e con altri atti di diritto derivato, sta adottando strumenti giuridici che permettono di gestire e valutare i rischi che le nuove tecnologie pongono al principio democratico ed ai diritti fondamentali. Siamo dunque di fronte all'emersione di un nuovo quadro giuridico, non solo europeo, che ha l'ambizione di anticipare le potenziali minacce per l'ordinamento democratico che possono provenire dall'utilizzo delle nuove tecnologie. L'emersione di questo quadro giuridico, tuttavia, anziché dare delle risposte chiare, sembra piuttosto lasciare aperte ancora molte domande.

Abstract (eng)

International organizations, like the Council of Europe, are adopting legal instruments that allow the development of an AI that does not enter in conflict with democracy and fundamental rights. The EU, with the AI Act as well as with other secondary Union legislation, is also adopting legal instruments that allow to manage and assess the risks posed by technological innovations to democracy and fundamental rights. We are thus witnessing the emersion of a new ambitious legal framework that wishes to prevent potential threats to democracy and fundamental rights coming from technological innovations. The emersion of such a legal framework, however, creates more questions than answers.

L'*AI ACT* E L'OBIETTIVO (MANCATO?) DI PROMUOVERE UNO STANDARD GLOBALE PER LA TUTELA DEI DIRITTI FONDAMENTALI

Enza Cirone[*]

SOMMARIO: 1. Introduzione. – 2. *AI Act*: un quadro d'insieme. – 3. Un approccio basato sul rischio: «*The difference between reality and fiction? Fiction has to make sense*». – 4. Quale ruolo per i diritti fondamentali? – 5. Prime osservazioni conclusive.

1. *Introduzione*

La regolamentazione dell'intelligenza artificiale ("IA") rappresenta da tempo una delle priorità del legislatore europeo[1]. Il dibattito su questo tema è sempre più fervente, in virtù sia dell'inarrestabile progresso della tecnologia, sia dell'intensificarsi della produzione normativa in questo ambito.

Così come già avvenuto con il regolamento europeo sulla protezione dei dati personali ("*GDPR*")[2], l'Unione europea è stata una pioniera nell'adottare il regolamento 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (d'ora in avanti, *AI Act*)[3], con l'intento altresì di rafforzare la propria reputazione di "legislatore globale"[4] nel contesto digitale.

[*] Assegnista di ricerca in diritto dell'Unione europea, Università degli Studi di Firenze.

[1] Si veda come esempio, Commissione europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM (2020) 65final, 19 febbraio 2020 e comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Promuovere un approccio europeo all'intelligenza artificiale, COM (2021) 205final, del 21 aprile 2021.

[2] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[3] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

[4] Come ben espresso da A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, n. 15, 14 marzo 2023, p. 325 «[L']ampia attività propositiva fa apparire oggi l'Unione

La proposta della Commissione di un regolamento "che stabilisce regole armonizzate sull'intelligenza artificiale (cd. legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione" è stata pubblicata il 21 aprile 2021[5], seguita dall'orientamento generale del Consiglio il 6 dicembre 2022[6] e dalla posizione negoziale del Parlamento europeo il 14 giugno 2023[7]. Nel dicembre 2023 il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sul testo dell'*AI Act* che è stato approvato dal Parlamento europeo nel marzo di quest'anno e che è stato sottoposto alla verifica finale dei giuristi-linguisti[8].

L'*AI Act* è uno strumento giuridico orizzontale che mira a promuovere l'adozione di sistemi di intelligenza artificiale incentrati sull'uomo, affidabili e che garantiscano un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, sanciti dalla Carta dei diritti fondamentali, compresi la democrazia, lo stato di diritto e la protezione dell'ambiente[9].

Il quadro normativo delineato segue un approccio basato sul rischio, non stabilendo regole uniformi per tutti i sistemi di intelligenza artificiale, bensì delineando diversi assetti giuridici. Ciascuno di questi sistemi individua obblighi giuridici correlati a rischi per gli interessi pubblici e per i valori e i diritti fondamentali protetti dall'ordinamento giuridico europeo. L'obiettivo, non solo dichiarato (ma anche esaltato) dal legislatore dell'Unione, è di garantire lo sviluppo, la diffusione e la *governance* responsabile dei sistemi di IA nell'UE, stabilendo regole precise, proteggendo i diritti fondamentali[10] e la sicurezza e promuovendo al contempo l'innovazione.

L'ambizioso progetto che il legislatore europeo ha cercato di realizzare è ora in una prima (connaturale) fase "di attenta analisi", in particolare dei suoi possibili (e talvolta fortemente auspicati) effetti e implicazioni in vari ambiti[11]. Infatti, l'*AI Act* è al centro di una serie di importanti quesiti che

come una sorta di laboratorio in cui si ricercano e sperimentano nuovi modelli normativi, volti a governare le trasformazioni tecnologiche in atto».

[5] COM (2021) 205final, cit.

[6] www.data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/it/pdf.

[7] www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.pdf.

[8] www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.

[9] V. considerando n. 1.

[10] Sul punto, si rimanda alle considerazioni svolte da C. Schepisi, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, pp. 53-75.

[11] Per un'analisi dei poteri normativi della Commissione europea e dei meccanismi sanzionatori previsti dall'*AI Act*, si rimanda al contributo di F. Ferri, *Il giorno dopo la rivoluzio-*

riguardano, tra gli altri, proprio la capacità di questo strumento giuridico interno all'ordinamento dell'Unione di avere un *reale e concreto* impatto sulla diffusione dei valori europei a livello *globale.*

La recente (e fruttuosa[12]) storia del *GDPR* inevitabilmente induce a riflettere sull'eventuale ruolo che il cd. effetto Bruxelles[13] potrebbe svolgere con riferimento all'*AI Act*. In virtù di questo meccanismo, da una parte, le imprese di tutto il mondo, anche se non soggette all'applicazione della normativa di riferimento, decidono autonomamente di attenersi ai (più rigorosi) standard europei nelle loro operazioni globali, e dall'altra, le giurisdizioni di Paesi terzi decidono spontaneamente di modellare le proprie normative interne sulla base dell'approccio europeo.

Prima di addentrarsi in qualsiasi considerazione riguardo alla portata dell'effetto Bruxelles, è *in primis* opportuno verificare se *l'AI Act* sia effettivamente riuscito nell'intento di affermare un "*gold standard*" per la tutela dei diritti fondamentali o se questo obiettivo sia passato in secondo piano, oscurato dall'esigenza primaria di garantire la sicurezza dei prodotti basati su intelligenza artificiale o, ancora, se questi due obiettivi siano adeguatamente bilanciati.

All'interno dell'*AI Act*, i riferimenti ai diritti fondamentali sono molteplici e questo *leitmotiv* risulta giustificato proprio dalle peculiarità dei sistemi di intelligenza artificiale[14] che, per loro natura, possono avere un notevole impatto sui diritti fondamentali e, in generale, sulla dimensione prettamente etica.

La duplice veste e finalità dell'*AI Act* – di promozione dell'innovazione e di tutela dei diritti fondamentali – si riflette, invero, nella sua duplice base giuridica[15], l'articolo 114 TFUE, disposizione che consente di adottare

ne: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea, in questo *fascicolo speciale*.

[12] Sulle difficoltà di *enforcement* del *GDPR* si rimanda a G. GENTILE, O. LYNSKEY, *Deficient by design? The transnational enforcement of the GDPR*, in *International & Comparative Law Quarterly*, 2022, pp. 799-830.

[13] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

[14] «L'utilizzo dell'IA con le sue caratteristiche specifiche (ad esempio opacità, complessità, dipendenza dai dati, comportamento autonomo) può incidere negativamente su una serie di diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ("la Carta")». V. paragrafo 3.5. della Relazione di accompagnamento della 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.

[15] Sul punto, si rimanda al contributo di M. INGLESE, *Il regolamento sull'intelligenza ar-*

misure volte al ravvicinamento delle normative nazionali relative all'instaurazione e al funzionamento del mercato interno, e l'articolo 16 TFUE[16], che consente all'Unione di adottare atti legislativi in materia di protezione dei dati personali[17].

Il presente contributo, dopo aver svolto qualche considerazione generale sull'*AI Act* (paragrafo 2), si propone di illustrare le principali caratteristiche dell'approccio basato sul rischio che ne costituisce l'ossatura (paragrafo 3). Successivamente, il paragrafo 4 esaminerà il ruolo *effettivo* dei diritti fondamentali all'interno dell'*AI Act*, mentre il paragrafo 5 trarrà qualche preliminare considerazione conclusiva riguardo alle potenzialità di questo strumento giuridico di diventare uno standard a livello globale.

2. AI Act*: un quadro d'insieme*

Come già menzionato in precedenza, il regolamento sull'intelligenza artificiale ben riflette la dicotomia tra innovazione e regolazione che caratterizza il quadro normativo europeo in materia, sin dalle sue fasi preparatorie[18]. Da un lato, infatti, segue l'imperativo della creazione di un mercato unico per l'IA[19], volto a prevenirne la frammentazione e a fornire regole chiare per gli operatori del settore. Dall'altro, si propone di consentire l'accesso al mercato unico dell'UE esclusivamente ai sistemi di IA considerati affidabili e conformi ai valori europei, specialmente quelli che promuovono la prote-

tificiale come atto per il completamento e il buon funzionamento del mercato interno, in questo *fascicolo speciale*.

[16] È interessante notare che, all'interno del regolamento, non vengono distinte le disposizioni basate su una base giuridica da quelle che trovano fondamento nell'altra base giuridica. Il considerando n. 3 precisa che, nella misura in cui il regolamento contenga norme specifiche sulla protezione delle persone con riguardo al trattamento dei dati personali per quanto riguarda le restrizioni all'uso dei sistemi di IA, per l'identificazione biometrica a distanza ai fini dell'applicazione della legge, dell'uso di sistemi di IA per la valutazione del rischio delle persone fisiche, è opportuno basare il regolamento, per quanto riguarda tali norme specifiche, sull'articolo 16 del TFUE.

[17] Per quanto vi siano dei punti in comune, la situazione è diversa nel *GDPR*, che si basa esclusivamente sull'articolo 16 TFUE e non sull'articolo 114 TFUE. L'articolo 16, infatti, rimanda al diritto fondamentale alla protezione dei dati che trova espressione nell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea.

[18] Cfr. comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa, COM (2018) 237final, del 25 aprile 2018; COM (2020) 65final, cit.

[19] Considerando n. 5.

zione dei diritti fondamentali, in quanto sistemi in grado di favorire lo sviluppo *antropocentrico* della tecnologia, ovvero sistemi in cui i diritti umani costituiscano il baricentro dell'intero asse.

Pur nel rispetto dei limiti delle competenze conferitele dai Trattati, l'Unione europea ha concepito il regolamento sull'intelligenza artificiale come uno strumento orizzontale, vale a dire una normativa che si applica a tutti i sistemi di IA. Poiché la protezione dei diritti fondamentali non può costituire da sola una base normativa, la tutela di tali diritti è integrata nell'ampia (e, per certi versi, controversa[20]) base giuridica fornita dall'articolo 114 TFUE[21], che disciplina l'armonizzazione delle norme relative al mercato interno[22].

Di conseguenza, il regolamento sull'intelligenza artificiale risulta uno strumento che, pur favorendo l'integrazione nell'ambito del mercato unico, adotta un approccio specifico (*rectius*, peculiare): garantisce certezza giuridica traendo ispirazione dalla regolamentazione della sicurezza dei prodotti[23] – beneficiando di decenni di esperienza acquisita con tali strumenti che sono diventati uno standard globale – e, al contempo, inserisce in tale cornice giuridica la tutela dei diritti fondamentali come requisito essenziale di *compliance*.

[20] Il campo di applicazione dell'art. 16 TFUE è limitato alla protezione dei dati personali, pertanto, risulta difficile individuare un diverso fondamento giuridico, tenute in considerazione le problematicità intrinseche del ricorso all'art. 352 TFUE in ragione del requisito dell'unanimità, come ben dimostra la situazione di stallo che caratterizza la proposta di direttiva orizzontale in materia di diritto antidiscriminatorio COM (2008) 426final, del 2 luglio 2008.

[21] L'attività normativa è fondata sull'esigenza di stabilire regole comuni ai fini del corretto funzionamento del mercato interno, si v. A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 27. In senso contrario, S. Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE*, n. 5, 20 dicembre 2021, pp. 69-84; Van Cleynenbreugel, *EU By-Design Regulation in the Algorithmic Society*, in AA.VV., *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

[22] Un atto legislativo basato sull'art. 114 TFUE deve avere un collegamento con l'obiettivo del ravvicinamento dei mercati. Per una disamina completa, si rimanda a S. Migliorini, *Il ravvicinamento delle legislazioni nella prospettiva del diritto dell'Unione europea e dei suoi effetti sul diritto interno. Le tecniche del ravvicinamento*, in *Osservatorio sulle fonti*, n. 3, 2012, pp. 1-18.

[23] Per approfondire il ragionamento seguito dalla Commissione europea riguardo la scelta di questa cornice giuridica, si veda: 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*, Milano, 2022, pp. 2-5.

Dalla proposta della Commissione europea, il testo dell'*AI Act* ha subito significative modifiche nell'*iter* di approvazione, configurandosi attualmente come un prodotto legislativo "ibrido" in cui la definizione di standard tecnici è collegata alla previsione di diritti e obblighi per gli sviluppatori dei sistemi di IA. Invero, la natura dinamica e complessa di questi sistemi ha richiesto una normativa più flessibile[24], con disposizioni meno prescrittive e più generiche, con il precipuo scopo di evitare di vincolare l'*AI Act* in maglie troppo strette, riducendo il rischio di renderlo rapidamente obsoleto e, di conseguenza, lasciando spazio (o piuttosto un onere) all'interpretazione giurisprudenziale. Ciononostante, può affermarsi che l'*AI Act* tuteli adeguatamente i diritti fondamentali?

Prima di rispondere a questa domanda, occorre innanzitutto precisare che, nella sua versione finale, l'*AI Act* garantisce uno spazio più significativo alla tutela dei diritti fondamentali rispetto alla proposta della Commissione; quest'ultima, infatti, muoveva dalla premessa che la legislazione sulla protezione dei consumatori già fornisse rimedi adeguati e che tali rimedi non rientrassero nella sfera della legislazione sull'armonizzazione tecnica. Mentre per i diritti, come ad esempio il diritto a ricevere spiegazioni sulle decisioni prese da un sistema di intelligenza artificiale, non ci sono novità sostanziali, trattandosi di un diritto che trovava già fondamento nell'articolo 22 del *GDPR*[25], per gli obblighi emergono, invece, importanti novità. Ad esempio, gli sviluppatori di sistemi di IA considerati ad alto rischio sono ora tenuti a condurre una valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*, di seguito "FRIA") prima di utilizzarli. Questa valutazione di impatto sui diritti fondamentali si differenzia dalla classica "cascata" di

[24] Si rileva che, ciononostante, alcuni commentatori, soprattutto dal mondo dell'industria, avevano sostenuto la necessità di includere la possibilità di aggiornare alcune definizioni e divieti tramite atti legislativi delegati. Con riferimento a ciò, occorre tenere in considerazione che, per definizione, gli atti legislativi delegati possono integrare o modificare determinati elementi non essenziali di un atto legislativo. Di conseguenza, sebbene la flessibilità sia un aspetto positivo in normative come quella in questione, non dovrebbe compromettere il principio democratico fondamentale che governa il procedimento legislativo europeo. È ipotizzabile che, ove necessario, modifiche specifiche ed essenziali potrebbero essere realizzate mediante un procedimento legislativo "accelerato".

[25] L'IA non è esplicitamente menzionata nel *GDPR*, tuttavia, la disposizione sulle decisioni automatizzate rileva come forma di controllo indiretto rispetto all'utilizzo dei sistemi di IA, sulla base della considerazione che tali sistemi sono frequentemente utilizzati per giungere a decisioni automatizzate che possono avere degli effetti sulle situazioni giuridiche soggettive degli individui.

obblighi degli operatori normalmente presenti nella legislazione sulla sicurezza dei prodotti, con il produttore – in questo caso, il fornitore – che detiene la maggior parte delle responsabilità, seguìto dall'importatore, dal distributore e, infine, dall'utente – ossia, l'utilizzatore – che non ha praticamente nessun obbligo.

3. *Un approccio basato sul rischio:* «The difference between reality and fiction? Fiction has to make sense»[26]

Riprendendo le considerazioni fatte poco sopra, merita ribadire che nel regolamento i sistemi di intelligenza artificiale sono disciplinati secondo un approccio basato sul rischio che comporta la loro classificazione in determinate categorie, all'interno delle quali sono incluse specifiche applicazioni di intelligenza artificiale.

Per chiarire visivamente la classificazione dei rischi e l'ampio spettro delle applicazioni di intelligenza artificiale soggette all'*AI Act*, la Commissione europea aveva ideato una rappresentazione grafica sotto forma di una piramide a quattro livelli[27] ciascuno dei quali colorato di colori diversi: la punta della piramide indicava i *rischi non accettabili,* a seguire vi era la porzione che rappresentava i *rischi elevati* (*high-risk*), al terzo livello i *rischi limitati* e, infine, nel segmento più in basso *i sistemi che presentavano rischi minimi o nessun rischio* (*minimal or no risk*).

In buona sostanza, al vertice della piramide erano indicate le applicazioni proibite a causa dei rischi inaccettabili per la salute, la sicurezza e i diritti fondamentali delle persone. Per la maggior parte dei sistemi di intelligenza artificiale, che non rappresentavano un rischio significativo solo per il loro utilizzo, non erano previste, già all'interno della proposta della Commissione, delle disposizioni specifiche, ma ne era disposta la gestione attraverso

[26] La citazione è attribuita a T. Clancy e, ad avviso dell'Autrice, ben riflette la *ratio* dell'approccio basato sul rischio (*Reader's Digest Quotable Quotes: Wit and Wisdom for All Occasions, Reader's Digest Association*, New York, 1997, p. 140).

[27] Nel 2021 la Commissione ha ideato una piramide su quattro livelli per illustrare la logica alla base della proposta di regolamento sull'IA, sottolineando il suo approccio basato sul rischio. Oltre ad essere stata utilizzata dai membri della Commissione in vari *workshop* di presentazione della normativa, come ad esempio nell'ambito del CEPS webinar – *European approach to the regulation of artificial intelligence*, 23 April 2021, www.ceps.eu/wp-content/uploads/2021/04/AI-Presentation-CEPS-Webinar-L.-Sioli-23.4.21.pdf, la piramide è pubblicata sul sito web della Commissione, www.digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

codici di condotta volontari. Al contrario, il regolamento, così come la proposta, dedica la maggior parte delle disposizioni sostanziali alle applicazioni ritenute ad alto rischio per la salute, la sicurezza e i diritti fondamentali. Tali sistemi sono disciplinati da norme derivate dal nuovo quadro legislativo per la sicurezza dei prodotti[28]. In base a tale approccio, i fornitori di sistemi di IA devono garantire che siano soddisfatti specifici requisiti tecnici prima di autorizzare l'immissione di tali sistemi nel mercato unico dell'UE, la messa in servizio o, in generale, l'utilizzo. I fornitori stessi di solito valutano la conformità a tali requisiti attraverso controlli interni, ma talvolta può essere richiesta una valutazione esterna. Infatti, anche se i controlli interni potrebbero essere sufficienti in base al dettato normativo, i fornitori potrebbero tuttavia trovarsi a dover ricorrere a forme esterne di convalida, come i meccanismi di certificazione o la conformità a standard tecnici armonizzati sviluppati dalle organizzazioni di standardizzazione[29], a seguito di una richiesta della Commissione europea, per garantire la piena copertura dei requisiti legali, che forniscono descrizioni astratte dei risultati che le misure tecniche devono garantire.

Nel testo originario della proposta della Commissione, il profilo di rischio di un sistema di IA si basava sull'applicazione prevista. Tuttavia, tale previsione non era adatta a modelli che possono essere utilizzati per una vasta gamma di compiti, come i *large language models*, perché questi possono essere integrati in una serie di sistemi e applicazioni a valle. In tali circostanze, il fornitore del sistema di IA sarebbe colui che utilizza il sistema generale per uno scopo specifico. Pertanto, l'efficacia dei requisiti tecnici dipenderebbe dalle decisioni tecniche prese dal fornitore del sistema generale, che potrebbe tenere in considerazione esclusivamente i rischi per la sicurezza e la salute, non includendo considerazioni inerenti al pericolo per i diritti fondamentali.

[28] Il nuovo quadro legislativo è stato introdotto nel 2008 con il regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 che ha segnato una nuova tappa fondamentale per il mercato interno. L'obiettivo del regolamento era di incrementare l'efficacia del sistema normativo attraverso un potenziamento del controllo, sia preventivo da parte degli organismi notificati, sia successivo da parte delle autorità di vigilanza, sulla conformità alla legislazione UE da parte degli operatori economici. Inoltre, il regolamento UE sulla standardizzazione dà facoltà alla Commissione europea di richiedere agli Organismi Europei di Normazione la creazione di "documenti di sicurezza".

[29] Sul punto, si rimanda al paragrafo 4 del presente contributo.

In tale contesto, la commercializzazione di Chat GPT, di proprietà della società statunitense Open AI, ha indotto a ripensare a queste tipologie di sistemi di IA che non erano stati adeguatamente contemplati nella bozza del regolamento.

Nel testo finale dell'*AI Act* sono state inserite norme specifiche per i sistemi di IA "per scopi generali" ("GPAI")[30]. Inoltre, il nuovo testo ha in-

[30] «La nozione di modelli di IA per finalità generali dovrebbe essere chiaramente definita e distinta dalla nozione di sistemi di IA per consentire la certezza del diritto. La definizione dovrebbe basarsi sulle principali caratteristiche funzionali di un modello di IA per finalità generali, in particolare la generalità e la capacità di svolgere con competenza un'ampia gamma di compiti distinti. Questi modelli sono solitamente addestrati su grandi quantità di dati con diversi metodi, come l'apprendimento autosupervisionato, non supervisionato o per rinforzo. I modelli di IA per finalità generali possono essere immessi sul mercato in vari modi, tra cui biblioteche, interfacce di programmazione delle applicazioni (API), download diretto o copia fisica. Tali modelli possono essere ulteriormente modificati o perfezionati con nuovi modelli. Sebbene i modelli di IA siano componenti essenziali dei sistemi di IA, essi non costituiscono di per sé sistemi di IA. I modelli di IA necessitano dell'aggiunta di altri componenti, ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte. Il presente regolamento stabilisce norme specifiche per i modelli di IA per finalità generali e per i modelli di IA per finalità generali che presentano rischi sistemici, le quali dovrebbero applicarsi anche quando tali modelli sono integrati o fanno parte di un sistema di IA. Resta inteso che gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero applicarsi una volta che i modelli di IA per finalità generali sono immessi sul mercato.» (considerando n. 97 *AI Act*). Inoltre, l'art. 3 (63) del regolamento definisce il "modello di IA per finalità generali" come un «modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

trodotto la classificazione di "rischio sistemico"[31] per questi modelli[32], che si verifica quando sono presenti determinate condizioni[33].

A tal riguardo, viene da domandarsi se la struttura piramidale ideata dalla Commissione subito dopo la pubblicazione della proposta di regolamento possa dirsi ancora attuale, considerata l'introduzione di questa ulteriore classificazione. Per quanto il dubbio possa dirsi lecito, si ritiene che

[31] L'art. 3 (65) definisce il rischio sistemico come «un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore». Per un approfondimento, v. C. KUTTERER, *Regulating Foundation Models in the AI Act: From "High" to "Systemic" Risk*, in *AI Regulation Papers*,www.ai-regulation.com/wp-content/uploads/2024/01/C-Kutterer-Regulating-Foundation-Models-in-the-AI.pdf.

[32] Nell'adozione del suo approccio generale, il Consiglio aveva proposto di aggiungere un nuovo breve titolo alla bozza della Commissione per includere le situazioni in cui i sistemi di IA possono essere utilizzati per molti scopi generali. Tuttavia, come detto sopra, l'introduzione nel mercato del modello di Open AI – ChatGPT – ha spinto il Parlamento a riconoscere l'urgente necessità di misure normative più sostanziali, portando all'inclusione delle GPAI all'interno dell'*AI Act* come risposta ai progressi tecnologici e ai rischi potenziali (www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html). Si consideri che, anche prima dell'emergere dei GPAI, il Consiglio aveva evidenziato la necessità di tenere in considerazione l'opacità, complessità, la presenza di *bias* e di imprevedibilità e di parziale automatismo del comportamento di alcuni sistemi di intelligenza artificiale, al fine di assicurarne la compatibilità con i diritti fondamentali e facilitare il rispetto delle regole (*Explanatory Memorandum of the AI Act Proposal*, Section 1, point 1.1).

[33] Innanzitutto, (i) il modello ha elevate capacità di impatto valutate sulla base di strumenti e metodologie tecniche adeguate, compresi indicatori e parametri di riferimento (che dovranno essere definiti con atti delegati della Commissione Europea); (ii) vi è una decisione della Commissione, d'ufficio o a seguito di una segnalazione da parte del gruppo scientifico, secondo cui un modello di AI per uso generale ha capacità o impatto equivalenti a quelli di cui alla lettera a).

La designazione come sistema GPAI a rischio sistemico viene svolta dalla Commissione Europea o sulla base della dichiarazione del produttore o d'ufficio secondo una procedura che ricalca quelle già disciplinate nel Digital Service Act e nel Digital Markets Act (art. 51, par.1, lett. b). Nel momento in cui il modello è classificato come a rischio sistemico sono inseriti ulteriori obblighi per i fornitori: (i) eseguire la valutazione del modello al fine di identificare e mitigare il rischio sistemico; (ii) valutare e mitigare i possibili rischi sistemici a livello dell'Unione, comprese le loro fonti; (iii) tenere traccia, documentare e riferire senza indebiti ritardi all'Ufficio AI e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti sugli incidenti gravi e le possibili misure correttive per affrontarli; (iv) garantire un livello adeguato di protezione della cybersecurity per il modello e per l'infrastruttura fisica del modello.

sia proprio la trasposizione del concetto di "rischio sistemico" nell'*AI Act* a permettere di preservare la struttura a piramide – e, più in generale, l'approccio basato sui livelli di rischio[34].

4 *Il ruolo dei diritti fondamentali nell'*AI Act

Nell'*AI Act*, i diritti fondamentali sono indicati come "interessi pubblici[35]" da proteggere assieme alla salute e alla sicurezza, all'interno del più ampio e generale contesto della tutela della sicurezza dei prodotti che si è detto aver ispirato il regolamento. Tale previsione non è certamente sorprendente, sia perché, in generale, il legislatore europeo è tenuto al rispetto dei diritti fondamentali nell'esercizio delle competenze che gli sono conferite dai Trattati, sia perché vi sono altri esempi di legislazioni orizzontali sulla sicurezza dei prodotti che includono la tutela dei diritti fondamentali tra i loro obiettivi[36].

Ciononostante, l'*AI Act* si distingue dalle precedenti normative in quanto nel regolamento la tutela dei diritti fondamentali costituisce, assieme alla previsione di standard tecnici, lo scheletro dell'intero impianto normativo e non, invece, uno dei vari requisiti da rispettare. Il rischio per i diritti fondamentali diventa, infatti, il principale criterio per la previsione di obblighi più stringenti.

Questa caratteristica distintiva del regolamento emerge chiaramen-

[34] Per interessanti e approfondite considerazioni sulla collocazione dei GPAI nel sistema piramidale dei rischi individuati dalla Commissione, si rimanda a T. Christakis, T. Karathanasis, *Tools for navigating the EU AI ACT: (2) Visualisation pyramid*, 7 March 2024, wwww.ai-regulation.com/visualisation-pyramid/.

[35] V. considerando n. 7.

[36] Ne è un esempio la normativa sui dispositivi medici. In particolare, il considerando n. 89 del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio precisa che: «Il presente regolamento rispetta i diritti fondamentali e i principi riconosciuti, in particolare, dalla Carta e, segnatamente, la dignità umana, l'integrità della persona, la protezione dei dati di carattere personale, la libertà delle arti e delle scienze, la libertà d'impresa e il diritto di proprietà. Gli Stati membri dovrebbero applicare il presente regolamento osservando tali diritti e principi». Merita soprattutto osservare che il regolamento fa esplicito riferimento alla protezione dei dati personali, includendo anche garanzie aggiuntive per la libertà di espressione (considerando n. 69) e la libertà di stampa (art.1, paragrafo 16).

te dai requisiti pratici che impone ai sistemi di IA: la valutazione dei rischi per i diritti fondamentali è equiparata a quella per la salute e la sicurezza, quest'ultimi sicuramente più comuni nel contesto della sicurezza dei prodotti[37]. In modo più specifico, l'*AI Act* stabilisce che, quanto maggiore è l'impatto negativo di un sistema di intelligenza artificiale sui diritti fondamentali garantiti dalla Carta, tanto più questo costituisce un criterio essenziale per la classificazione di una applicazione come di rischio elevato.

Come già precisato in precedenza, i diritti fondamentali non erano così centrali all'interno della proposta della Commissione[38]; tuttavia, nonostante la loro rilevanza nell'attuale testo del regolamento, l'aspetto della tutela dei diritti rimane quello più controverso.

Le critiche concernono essenzialmente due questioni: da una parte, lo stretto – e per certi versi inscindibile – legame tra i diritti fondamentali e gli strumenti propri della regolamentazione sulla sicurezza dei prodotti e, dall'altra, la formulazione troppo ampia e vaga della maggior parte delle disposizioni che riguardano i sistemi di IA ad alto rischio.

In merito al primo nodo[39], ciò che viene particolarmente contestato è la probabilità che la valutazione del rischio per i diritti fondamentali segua

[37] Tale previsione riflette l'importanza centrale dei diritti fondamentali nell'ordinamento giuridico europeo e, in particolare, della Carta dei diritti fondamentali in quanto fonte di diritto primario nel sistema costituzionale europeo.

[38] È interessante notare che, proprio in risposta alle critiche rivolte alla proposta della Commissione rispetto al ruolo secondario dei diritti fondamentali, il Parlamento europeo ha introdotto significative modifiche al regolamento, come l'introduzione del diritto di ottenere una spiegazione per coloro che sono interessati da decisioni basate su sistemi di IA ad alto rischio. Da ultimo, un ulteriore emendamento ha riguardato l'inclusione di nuovi valori da tutelare, ovvero la democrazia, lo stato di diritto e l'ambiente che si sono sommati a quelli già indicati, "salute, sicurezza e diritti fondamentali". Si veda: considerando n. 1, *Emendamenti del Parlamento europeo, approvati il 14 giugno 2023, alla 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,* (P9_TA(2023)0236): «Lo scopo del presente regolamento è promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile e garantire un livello elevato di protezione della salute, della sicurezza, dei diritti fondamentali, della democrazia e dello Stato di diritto, nonché dell'ambiente, dagli effetti nocivi dei sistemi di intelligenza artificiale nell'Unione, sostenendo nel contempo l'innovazione e migliorando il funzionamento del mercato interno».

[39] Per approfondire, si rimanda a A. Mantelero, *Beyond data: Human rights, ethical and social impact assessment in AI*, in *Information Technology and Law Series*, 2022; S. Palmieri, T. Goffin, *A blanket that leaves the feet cold: exploring the AI Act Safety Framework for Medical AI*, in *European Journal of Health Law*, 2023, p. 406.

gli stessi metodi di valutazione del rischio utilizzati per la sicurezza dei prodotti[40], aumentando così il pericolo di negligenza nella protezione dei diritti fondamentali[41]. Infatti, a differenza del settore della sicurezza dei prodotti, dove il rischio può essere quantificato mediante calcoli computazionali[42], per i diritti fondamentali non è possibile riferirsi a mere valutazioni numeriche.

A tal riguardo, ci si domanda se l'introduzione della valutazione di impatto per i diritti fondamentali possa arginare, almeno in parte, questi pericoli. In base all'articolo 27 del regolamento, è richiesto che, prima di utilizzare un sistema di IA ad alto rischio, gli utilizzatori valutino se l'impiego di tale sistema potrebbe comportare un pregiudizio per i diritti fondamentali.

L'introduzione della FRIA è stata fortemente sostenuta dal Parlamento europeo che riteneva che questo importante emendamento potesse contribuire a consolidare l'obiettivo di una IA antropocentrica, garantendo il rispetto della protezione dei diritti fondamentali nel contesto dell'*AI Act*. Tuttavia, nonostante questi buoni propositi, una prima analisi delle disposizioni rilevanti porta a rilevare innanzitutto che la FRIA non sembra essere stata pienamente integrata nel quadro normativo del regolamento, mettendo ancor più in luce come questa integrazione sia stata frutto di un compromesso politico, nell'ambito del quale molti degli elementi chiave per una strutturata e adeguata valutazione di impatto sui diritti fondamentali sono stati omessi[43].

In questo contesto, vale la pena precisare che l'approccio basato sul rischio adottato nell'*AI Act* differisce da quello adottato dal *GDPR*, nel quale i diritti fondamentali sono centrali, e un rischio elevato, salvo che sia giustificato da interessi prevalenti, costituisce un limite non superabile[44]. Nell'*AI Act* che, invece, ha un ambito di applicazione più ampio e un duplice fondamento giuridico, il criterio di riferimento è quello della accettabilità del

[40] A tal riguardo, si noti che l'art. 3 (2) definisce il rischio come «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso».

[41] Il rischio per i diritti fondamentali potrebbe derivare da pericoli che non appaiono di per sé tali, v. L. HIN-YAN ET AL., *Governing boring apocalypses: A new typology of existential vulnerabilities and exposures for existential risk research*, in *Futures*, 2018, p. 6.

[42] M. HILDEBRANDT, *Privacy as Protection of the incomputable self: from agnostic to agnostic machine learning*, in *Theoretical Inquiries Law*, 2019, p. 23.

[43] Sul punto, si rimanda all'approfondita analisi di M. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template*, 2024, www.papers.ssrn.com/sol3/papers.cfm?abstract_id=4782126.

[44] Si v. art. 35 *GDPR*; E. COSTA, *Data protection impact assessment*, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY (eds.), *The EU General Data Protection Regulation (GDPR) – A Commentary*, Oxford, 2020, pp. 665-679.

rischio che, in prima battuta, pare contrastare con la visione antropocentrica dell'assetto normativo europeo sull'intelligenza artificiale. Tuttavia, dato che l'articolo 27 dell'*AI Act* non fa mai riferimento alla "accettabilità" del rischio, si può ragionevolmente dedurre che il potenziale rischio elevato di pregiudizio per i diritti fondamentali derivante dall'uso di sistemi di IA ad alto rischio non possa considerarsi, in termini generali, accettabile.

Malgrado ciò, i tempi non sono maturi per affermare con certezza che questo strumento si rivelerà inefficace o che, al contrario, rappresenterà un rimedio alle lacune intrinseche al regolamento che, come si è detto, derivano direttamente dal suo impianto strutturale.

Come anticipato, l'altro punto di attenzione, oggetto di ampie critiche, concerne la formulazione – in maniera ampia e astratta – delle principali disposizioni riguardanti i sistemi ad alto rischio, il che implica inevitabilmente un ricorso a norme tecniche armonizzate[45] e a meccanismi di certificazione per interpretarle[46]. Nonostante siano senza dubbio utili, tali strumenti sfuggono al processo legislativo[47] in quanto sono appannaggio di soggetti privati. Pertanto, viene da domandarsi se sia appropriato affidare a tali

[45] L'art. 3 (27) dell'*AI Act* richiama la definizione dell'art. 2 (1) (c) del regolamento 1025/2012, ovvero «una norma europea adottata sulla base di una richiesta della Commissione ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione».

[46] Si rimanda a M. Eliantonio, A. Volpato, *The Participation of Civil Society in ETSI from the Perspective of Throughput Legitimacy*, in *Innovation: The European Journal of Social Science Research*, 2024, pp. 1-17 per una interessante analisi della recente riforma del modello di governance di ETSI. Per una panoramica più generale della questione, si suggerisce la lettura di M. Eliantonio, C. Cauffman (eds.), *The legitimacy of standardisation as a regulatory technique in the EU*, Cheltenham, 2020.

[47] In questo contesto, è importante notare che il processo di adozione degli standard non gode della stessa apertura e trasparenza del processo legislativo. Le discrepanze sono evidenti: manca il rispetto del principio democratico, la rappresentanza della società civile non è completa e soltanto i riferimenti agli standard vengono pubblicati sulla Gazzetta ufficiale. Proprio con riferimento a quest'ultimo aspetto, si noti che il Tribunale dell'Unione europea si è pronunciato nell'ambito di un ricorso in annullamento riguardante il rifiuto della Commissione europea di garantire accesso libero e gratuito a una Organizzazione no profit a degli standard adottati dal CEN nell'ambito della sicurezza dei giocattoli. In particolare, al paragrafo 107 il Tribunale ha precisato: « […]a parte il fatto che le ricorrenti non indicano la fonte esatta di un «principio costituzionale» che postulerebbe un accesso libero e gratuito alle norme armonizzate, esse non giustificano in alcun modo perché tali norme debbano essere soggette all'obbligo di pubblicità e di accessibilità connesso ad una «legge», in quanto tali norme non sono vincolanti, producono gli effetti giuridici ad esse connessi solo nei confronti degli interessati e possono essere consultate gratuitamente in alcune biblioteche degli Stati membri». (Tribunale 14 luglio 2021, causa T-185/19, *Public.Resource.Org e Right to Know/Commissione*).

organizzazioni la definizione di norme concernenti la protezione dei diritti fondamentali[48] che sono certamente essenziali per l'obiettivo perseguito dal regolamento.

I critici più aspri[49] sostengono che, in questo modo, il legislatore europeo stia delegando a enti privati la responsabilità di redigere normative in materia di diritti fondamentali[50] (occorre infatti considerare che si tratta di normative vincolanti e non di *soft law*!). In buona sostanza, queste critiche riflettono, non solo la considerazione della probabile incompetenza di questi enti a regolamentare la materia dei diritti fondamentali ma, dall'altra, anche la già menzionata preoccupazione che gli standard abbiano una carenza di legittimità democratica, mettendo in discussione la loro capacità di regolare adeguatamente i diritti fondamentali[51].

[48] Art. 40 (3) *AI Act*: «I partecipanti al processo di normazione cercano di promuovere gli investimenti e l'innovazione nell'IA, anche mediante una maggiore certezza del diritto, nonché la competitività e la crescita del mercato dell'Unione, contribuiscono a rafforzare la cooperazione globale in materia di normazione e a tenere conto delle norme internazionali esistenti nel settore dell'IA che sono coerenti con i valori, i diritti fondamentali e gli interessi dell'Unione e rafforzano la governance multipartecipativa garantendo una rappresentanza equilibrata degli interessi e l'effettiva partecipazione di tutti i portatori di interessi pertinenti conformemente agli articoli 5, 6 e 7 del regolamento (UE) n. 1025/2012». A tal riguardo, vale la pena precisare che, ai sensi dell'art. 41 (1) (iii) dell'*AI Act*, la Commissione può adottare atti di esecuzione per introdurre norme comuni per i sistemi ad altro rischio in determinate ipotesi, tra le quali, ad esempio, il caso in cui le norme tecniche armonizzate non affrontino adeguatamente le preoccupazioni per i diritti fondamentali.

[49] Ada Lovelace Institute, *Inclusive AI governance: civil society participation in standards development*, 2023, www.adalovelaceinstitute.org/report/inclusiveai-governance; C. H. Hofmann, *The Integration of Global Standards into the EU as regulatory Union*, in *University of Luxembourg Law Research Paper*, 7 October 2022; H.-W. Micklitz, R. Van Gestel, *European Integration through Standardization: How Judicial Review is Breaking Down the Club House of Private Standardization Bodies*, in *CMLR*, 2013, pp. 145-181.

[50] Secondo l'EDRI, i diritti fondamentali sono evidentemente al di là delle competenze e dell'autorità delle organizzazioni europee di standardizzazione e non dovrebbero essere sottoposti a standardizzazione tecnica. Si rimanda a: EDRI, *The Role of Standards and Standardisation Processes in the EU's Artificial Intelligence (AI) Act*, www.edri.org/wp-content/uploads/2022/05/The-role-of-standards-and-standardisation-processes-in-the-EUs-Artificial-Intelligence-AI-Act.pdf.

[51] Sul punto, si precisa che gli standard armonizzati sono particolarmente valorizzati nell'Unione europea, specialmente nei settori tecnici. A questo proposito, la CGUE ha chiarito che le norme tecniche formulate da enti di normazione come l'ISO, e rese obbligatorie tramite una normativa dell'Unione, diventano vincolanti per il pubblico generale solo se pubblicate nella Gazzetta ufficiale dell'Unione europea. Tuttavia, la Corte ha anche specificato che, nel caso in cui le aziende abbiano accesso alla versione ufficiale e autenticata di tali

Dato il contesto generale degli standard tecnici, inserire semplicemente considerazioni sulla tutela dei diritti fondamentali nella definizione degli stessi non è adeguato, almeno non dal punto di vista operativo. La questione del rispetto dei diritti fondamentali è intrinsecamente complessa e dipende dalle circostanze specifiche di ciascun caso. Di conseguenza, non può trattarsi di un processo svolto *una tantum*, né può dipendere dalla conformità a norme tecniche stabilite da uno standard perché, se così fosse, l'efficacia dell'intero sistema di IA potrebbe essere notevolmente messa a repentaglio[52].

5. *Prime osservazioni conclusive*

Dall'analisi svolta nei precedenti paragrafi è emerso che l'*AI Act* ha l'obiettivo non solo di raggiungere dei risultati in termini di posizionamento dell'Unione europea nel mercato mondiale delle soluzioni basate sull'intelligenza artificiale, ma anche di rendere l'Unione europea un *leader* globale in questo settore.

Tuttavia, si pone una questione cruciale: è possibile realizzare tali obiettivi se il regolamento non assicura un'adeguata protezione dei diritti fondamentali e dei valori?

Occorre innanzitutto osservare che, diffondere l'*AI Act* come modello di regolazione dell'intelligenza artificiale, non equivale automaticamente a rendere l'approccio europeo di regolazione dell'intelligenza artificiale uno standard riconosciuto (ed emulato) a livello globale, nonostante l'intenzione del legislatore europeo di conferire al regolamento un effetto extraterritoriale.

Da un'analisi preliminare, pare di poter affermare che l'*AI Act* sia in grado di essere esportato come modello di regolazione unico e "brevettato" – grazie all'*expertise* acquisita nel settore della sicurezza dei prodotti – essen-

norme, queste ultime assumono carattere vincolante per le aziende stesse (v., Corte giust. 22 febbraio 2022, C-160/20, *Stichting Rookpreventie Jeugd e a.*, punti 52 e 53). Inoltre, occorre rilevare che, nel contesto della protezione dei dati personali, sono stati adottati numerosi standard tecnici, che sono generalmente considerati come un importante requisito per la verifica della compliance al *GDPR*.

[52] Non è questa la sede per una disamina più ampia delle specificità delle norme tecniche armonizzate nel contesto dell'*AI Act*. Per un approfondimento, si rimanda a J. Laux, S. Watcher, B. Mittelstadt, *Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act*, in *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2024, pp. 1-11; M. Ho-Dac, *Considering Fundamental Rights in the European Standardisation of Artificial Intelligence: Nonsense or Strategic Alliance?*, in K. Jakobs (ed.), *Joint Proceedings EURAS & SIIT*, 2023.

do potenzialmente in grado di rispondere adeguatamente a problematiche di tipo regolatorio (il c.d. effetto Bruxelles *de iure*).

Tuttavia, l'*AI Act* non sembra che rifletta le caratteristiche essenziali per essere considerato uno standard globale, proprio in virtù del (solo formalmente centrale) ruolo della protezione dei diritti fondamentali nell'intera struttura del regolamento.

Dato l'obbligo "costituzionale" di promuovere i valori europei nell'azione esterna[53], assieme al dichiarato intento di diffondere il modello europeo di regolamentazione dell'IA oltre i confini europei, sarebbe stato opportuno attribuire un ruolo più rilevante ai diritti fondamentali in termini di *efficacia pratica.*

Sorprende, infatti, che l'*AI Act* legittimi paradossi come quello in virtù del quale sistemi di intelligenza artificiale sviluppati nell'Unione europea ma esportati oltre i confini europei, non rientrando nel campo di applicazione del regolamento, possano potenzialmente essere realizzati in violazione dei diritti fondamentali[54].

Gli effetti ambivalenti che emergono potrebbero derivare da diversi fattori convergenti. Tra questi, vi è senz'altro l'entusiasmo di aver introdotto la prima normativa orizzontale sull'IA che ha indubbiamente accelerato il processo di approvazione, soprattutto nelle ultime e più delicate fasi. Questo traguardo, se da un lato è motivo di orgoglio e prestigio[55], dall'altro può aver generato aspettative eccessive e un certo grado di pressione per produrre un regolamento all'altezza degli obiettivi annunciati. In aggiunta, come si è visto, l'adozione di un modello di tutela della sicurezza dei prodotti come base per la regolamentazione dell'IA potrebbe aver introdotto elementi di incertezza e inadeguatezza. Sebbene sia un approccio con radici solide, l'applicazione diretta di questo modello a un settore così complesso come l'IA potrebbe aver portato a lacune e incoerenze.

La complessità della situazione richiederà certamente un'analisi attenta e approfondita degli effetti del regolamento nel medio-lungo periodo. Solo così sarà possibile confermare o smentire le ipotesi formulate finora. Inoltre, la buona riuscita del nuovo quadro normativo dipenderà ampiamente anche

[53] Articolo 3 (5) e art. 21 TUE.

[54] Cfr. considerando n. 22.

[55] Si ricorda l'impegno delle istituzioni coinvolte nel procedimento legislativo ad adottare l'atto entro la fine della legislatura. Cfr. Dichiarazione comune del Parlamento europeo, del Consiglio dell'Unione europea e della Commissione europea, Priorità legislative dell'UE per il 2023 e il 2024, 2022/C 491/01.

dall'efficacia dei controlli da parte delle autorità competenti[56] e delle Istituzioni, in particolare la Commissione europea e la Corte di Giustizia, incaricate, rispettivamente, di garantire la corretta applicazione e interpretazione della normativa.

[56] Sul punto si rinvia al contributo di S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in questo *fascicolo speciale*.

Abstract (ita)

L'Unione europea è stata una pioniera nell'adozione di una normativa in materia di intelligenza artificiale ("IA"), con l'intento di consolidare la propria posizione come leader globale nella regolamentazione del settore digitale. Il presente contributo, dopo aver delineato le principali caratteristiche del quadro normativo europeo sull'IA, si propone di verificare se l'*AI Act* sia in grado di stabilire uno standard normativo globale per l'intelligenza artificiale e promuovere i valori europei oltre i confini dell'ordinamento giuridico europeo.

Abstract (eng)

The European Union has led the way in establishing legislation for artificial intelligence (AI) to position itself as a global leader in digital sector regulation. This paper outlines the critical elements of the European AI regulatory framework and investigates whether the AI Act can set a worldwide regulatory benchmark for artificial intelligence while promoting European values beyond the jurisdiction of the EU legal system.

IL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE COME ATTO PER IL COMPLETAMENTO E IL BUON FUNZIONAMENTO DEL MERCATO INTERNO?

Marco Inglese*

SOMMARIO: 1. Introduzione. – 2. La Strategia per il completamento del mercato unico digitale e il regolamento come strumento di armonizzazione. – 3. Basi giuridiche, armonizzazione, sussidiarietà, proporzionalità e diritti fondamentali: un facile bilanciamento? – 4. Osservazioni conclusive.

1. *Introduzione*

Il regolamento sull'intelligenza artificiale[1] (IA) ha, sin dai tempi della proposta di atto legislativo da parte della Commissione[2], attirato l'attenzione della dottrina. Esso, infatti, si inserisce in un quadro globale[3] e regionale[4] nel quale diversi attori – istituzioni, imprese, consumatori, comitati etici, gruppi di investimento, attivisti per i diritti digitali – si muovono per comprendere,

* Professore associato di Diritto dell'Unione europea presso l'Università di Parma, Dipartimento di Giurisprudenza, Studi politici e internazionali, Dipartimento di eccellenza 2023-2027. Il presente contributo rientra nelle attività del progetto *Human-Centered Approach and Regulatory Dimension in Developing an Interoperable and Secure Cyberspace* (HARD DISC), a sua volta parte del progetto *Security Rights in Cyber Space* (SERICS).

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

[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) 206final, 21 aprile 2021. A dispetto della traduzione ufficiale, ci si premura di sottolineare che la fonte *legge* non esiste nell'ordinamento giuridico dell'Unione europea.

[3] United Nations, General Assembly, Seventy-eight session, 11 March 2024, Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development, A/78/L.49.

[4] Council of Europe, 133rd Session of the Committee of Ministers, 17 May 2024, Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

da un lato, gli innegabili benefici dell'IA – ad esempio, in termini di velocizzazione dei processi decisionali e produttivi – e, dall'altro, i rischi che essa apporterebbe al godimento di taluni diritti fondamentali. Del resto, tali e tanti possono essere e, probabilmente, saranno gli effetti dell'IA sulla vita quotidiana degli individui che ne sono già stati minuziosamente esaminati i profili più eterogenei. Le posizioni emerse in letteratura – sulle quali si ritornerà anche *infra* – possono, sostanzialmente, suddividersi per comodità ma, naturalmente, senza pretesa di esaustività, valorizzando due approcci.

In primo luogo, alcuni autori hanno messo in evidenza come il diritto necessariamente segua, o meglio, *insegua*, le nuove tecnologie, sforzandosi di approntare soluzioni nuove a problemi prima inesplorati ovvero a saggiare se le categorie più consolidate – si pensi, ad esempio, alla tutela del consumatore nei contratti negoziati al di fuori dai locali commerciali o alle diverse forme di manifestazione del consenso – siano ancora in grado di reggere l'urto dell'innovazione. Più nello specifico, ne costituisce un esempio saliente la verifica dell'applicabilità della direttiva sui prodotti difettosi anche ai sistemi di IA[5].

In secondo luogo, altri autori si sono interrogati sulla tutela dei diritti fondamentali negli spazi digitali[6] per comprendere se, ed eventualmente, in che modo, l'IA rischi di comprimerli e, di conseguenza, come il legislatore debba intervenire in un difficile esercizio di bilanciamento, creando idonei spazi di salvaguardia[7].

[5] T. S. Cabral, *Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive*, in *MJECL*, 2020, p. 615 ss.; L. Belder, *Governance of Digital Technology: Towards Principles for the Regulation of the Design, Implementation and Monitoring of AI Systems*, in U. Bernitz, X. Groussot, J. Paju, S. A. De Vries (eds.), *General Principles of EU Law and the EU Digital Order*, Alphen den Rijn, 2020, p. 385 ss.

[6] A. Adinolfi, *Evoluzione tecnologica e diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, n. 15, 2023, p. 323 ss.

[7] In particolare, F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *DUE*, 2021, p. 454 ss.; F. Ferri, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *DUE*, 2022, p. 277 ss.; C. Grieco, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea*, Macerata, 2023; F. M. Mancioppi, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in *federalismi.it*, 2024, p. 112 ss.; G. Sartor, *Artificial Intelligence and Human Rights: Between Law and Ethics*, in *MJECL*, 2020, p. 705 ss.; C. Schepisi, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della* Commissione, in *I Post di AISDUE*, n. 16, 2022, p. 330 ss.; F. Ufert, *AI Regulation through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?*, in *EP*, 2020, p. 1087 ss.

Peraltro, è appena il caso di sottolineare che entrambi gli approcci contestualizzano l'IA nel più ampio piano di sviluppo dell'autonomia strategica e tecnologica dell'Unione – anche, ma non solo, nel settore della difesa[8] – soprattutto rispetto agli Stati Uniti e alla Cina, sottolineando la necessità di poderosi investimenti per recuperare il divario attualmente creatosi.

Partendo dal suesposto quadro dottrinale e muovendosi in assenza di prassi delle istituzioni nell'applicazione del regolamento IA e di giurisprudenza della Corte di giustizia nell'interpretazione dello stesso, il presente contributo intende assumere una posizione più modesta ma, cionondimeno, saldamente ancorata alle fondamenta dell'ordinamento giuridico dell'Unione. Infatti, è stato finora sottaciuto, a parte qualche rara eccezione[9], che il regolamento IA altro non sia che un classico atto di diritto derivato adottato per il ravvicinamento delle legislazioni, il completamento e il buon funzionamento del mercato interno, nella sua *species* di mercato unico digitale (MUD)[10]. In questo senso, sembra che l'orientamento del

[8] A Strategic Compass for Security and Defence for a European Union that Protects its Citizens, Values and Interests and Contributes to International Peace and Security, www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf. Il tema ha già attirato un interesse crescente in letteratura: C. Cellerino, *La difesa europea dinanzi alla guerra in Ucraina tra "autonomia strategica" e vincoli strutturali: quali prospettiva per la Difesa comune?*, in *DUE*, 2022, p. 9 ss.; P. De Pasquale, F. Ferraro, *L'autonomia strategica dell'Unione europea: dalla difesa… alla politica commerciale c'è ancora tanta strada da fare*, in *DPCE*, 2023, p. 5 ss.; G. Perotto, *The Legal Framework of the EU Defence Industry and the Pursuit of Strategic Autonomy*, in *EP*, 2023, p. 475 ss.; S. Poli, *Reinforcing Europe's Technologica Sovereignity throuh Trade Measures: The EU and Member States' Shared Sovereignnity*, in *EP*, 2023, p. 429 ss.

[9] S. De Vries, O. Kanevskaia, R. de Jager, *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, in *EP*, 2023, p. 583 ss.; S. De Vries, *Recent Trends in EU Internal Market Legislation. Bringing back the Old Concepts?*, in T. Van den Brink, V. Passalacqua (eds.), *Balancing Unity and Diversity in EU Legislation*, Cheltenham, 2024, p. 17 ss.

[10] Per quanto possano essere note le modifiche linguistiche e stilistiche del Trattato e della giurisprudenza che hanno portato alla trasformazione del mercato da comune a unico e, infine, interno, sembra opportuno richiamare come i tre aggettivi siano ormai usati in modo intercambiale. La prima definizione di mercato comune si rinviene in Corte giust. 5 maggio 1982, 15/81, *Schul*, punto 33 «la nozione di mercato comune, elaborata dalla Corte nella sua costante giurisprudenza, mira ad eliminare ogni intralcio per gli scambi intracomunitari al fine di fondere i mercati nazionali in un mercato unico il più possibile simile ad un vero e proprio mercato interno. È importante che i vantaggi di tale mercato siano garantiti, oltre che ai commercianti di professione, anche ai privati che si trovino a intraprendere operazioni commerciali oltre le frontiere nazionali». Innestandosi su questi presupposti, l'art. 26, par.

legislatore sia evidente fin dalla scelta della base giuridica, l'art. 114 TFUE[11], accompagnato dall'art. 16 TFUE, con il primo a fungere da centro di gravità rispetto al secondo[12].

Di conseguenza, il paragrafo 2 posiziona il regolamento sull'IA nella ormai decennale Strategia per il MUD[13], nella quale, originariamente non ve ne era traccia. È solo con la successiva revisione intermedia[14] che l'IA inizia ad essere considerata come un tema particolarmente sensibile da integrare nelle catene di valore della produzione; pertanto, l'Unione si propone di investire nella ricerca e nello sviluppo di sistemi innovativi di IA[15]. Inoltre, ci si interrogherà su alcuni profili critici relativi all'uso co-

2, TFUE lo definisce «uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni dei trattati». Per una ricostruzione, ormai di carattere storico ma sempre pertinente, si veda K. Mortelmans, *The Common Market, the Internal Market and the Single Market, What's in a Market?*, in *CMLR*, 1998, p. 101 ss. Per una ricostruzione più attuale, invece, S. Weatherill, *The Internal Market as a Legal Concept*, Oxford, 2016. Per quanto, ancora, concerne, alcune discrepanze nella giurisprudenza della Corte e i loro effetti sul legislatore e, di conseguenza, sulle tecniche regolatorie, J. Lindeboom, *Interpreting the EU Internal Market*, in F. Amtenbrink, G. Davies, D. Kochenov, J. Lindeboom (eds.), *The Internal Market and the Future of European Integration. Essays in Honour of Laurence W. Gormley*, Cambridge, 2019, p. 81 ss.

[11] Sull'art. 114 TFUE come base giuridica si richiama l'approfondito studio di T. M. Moschetta, *Il ravvicinamento delle normative nazionali per il mercato interno. Riflessioni sul sistema delle fonti alla luce dell'art. 114 TFUE*, Bari, 2018.

[12] La scelta del legislatore è, inoltre, evidenziata, in 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, SWD (2021)84. In particolare, «t[his] initiative constitutes a core part of the EU single market strategy» (p. 30) e *passim*, p. 31.

[13] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia per il mercato unico digitale in Europa, COM (2015) 192final, del 6 maggio 2015.

[14] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale, Un mercato unico digitale connesso per tutti, COM (2017) 228final, del 10 maggio 2017.

[15] Nel prosieguo della trattazione si farà particolare riferimento alle comunicazioni della Commissione che hanno preparato l'adozione degli atti legislativi volti a completare e garantire il buon funzionamento del MUD. Sul ruolo, invece, del Parlamento, si rinvia a G. Di Federico, *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. Di Federico (a cura di), *Alla (ri)scoperta del Parlamento europeo: 1979-2019*, Torino, 2021, p. 71 ss.

stante del regolamento come strumento privilegiato per l'armonizzazione nel MUD. Il paragrafo 3, invece, esamina più in dettaglio le caratteristiche essenziali del regolamento IA ponendo l'accento sui consolidati principi di sussidiarietà e proporzionalità che devono guidare l'Unione nell'esercizio di una competenza concorrente quale il mercato interno secondo l'art. 4, par. 2, lett. *a*), TFUE. Dunque, ci si soffermerà anche sul ruolo delle c.d. clausole trasversali[16] *ex* art. 10 e art. 12 TFUE concernenti, rispettivamente, il contrasto alle discriminazioni e la tutela dei consumatori. Peraltro, esse trovano ulteriore manifestazione anche nell'art. 21 e nell'art. 38 della Carta. Di conseguenza, si farà riferimento alla consolidata tecnica del bilanciamento nella misura in cui le potenziali esternalità negative dell'IA – si pensi, in prima battuta, alla discriminazione algoritmica o alla difficoltà di individuare il responsabile di un evento dannoso – devono essere internalizzate, tramite un atto di diritto derivato quale il regolamento in commento, attraverso il contemperamento di esigenze contrapposte. Non si tratta di una novità, anzi, nel tempo, ciò è andato affermandosi come la normalità dell'azione legislativa, in particolare nei settori che richiedono particolare cautela. Basti rammentare, a titolo di esempio, la direttiva sui prodotti del tabacco[17] e le esigenze di consentirne la libera circolazione nel rispetto della salute degli individui e, in particolar modo, delle fasce più vulnerabili, tra cui i minori. In conclusione, si sostiene che il regolamento IA ben si collochi nella più ampia (e ormai storica) rappresentazione del mercato interno dell'Unione, la quale si caratterizza, secondo l'art. 3 TUE[18], sia per «instaurar[lo]» sia per voler essere «una economia sociale di mercato fortemente competitiva» prestando attenzione, quindi, sia alle dinamiche di carattere economico-mercantilistico sia alla tutela dei diritti degli individui[19].

[16] Sulla proliferazione delle clausole trasversali, si rimanda integralmente a F. Ippolito, M. E. Bartoloni, M. Condinanzi (eds.), *The Proliferation of Integration Principles under the Treaty of Lisbon*, London-New York, 2014.

[17] Direttiva 2014/40/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, sul ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri relative alla lavorazione, alla presentazione e alla vendita dei prodotti del tabacco e dei prodotti correlati e che abroga la direttiva 2001/37/CE.

[18] I. Govaere, *Internal Market Dynamics: On Moving Targets, Shifting Contextual Factors and the Untapped Potential of Article 3(3) TEU*, in I. Govaere, S. Garben (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford, 2020, p. 75 ss.

[19] Soprattutto nell'ultima decade si è assistito a un rinnovato interesse verso la locuzione «economia sociale di mercato fortemente competitiva». Essa compare *verbatim* in numerose

2. *La Strategia per il completamento del mercato unico digitale e il regolamento come strumento di armonizzazione*

Pubblicata nel 2015, la Strategia per il completamento del MUD aveva un triplice obiettivo. Innanzitutto, la Commissione prevedeva l'adozione di un pacchetto molto eterogeneo di atti di diritto derivato volti a regolamentare il mercato digitale al fine di consentire la libera circolazione dei servizi, con una particolare attenzione anche alla tutela dei diritti degli individui, conscia che l'impeto dello sviluppo tecnologico stava già evidenziando i limiti degli atti giuridici al tempo in vigore. In seconda battuta, essa intendeva creare un *level playing field* in grado di stimolare la competitività delle imprese e attrarre nuovi investimenti. Da ultimo, occorreva prestare particolare attenzione al potenziale esacerbarsi di dinamiche anticoncorrenziali, soprattutto considerando la posizione di dominanza di alcune grandi imprese.

Come anticipato nel paragrafo precedente, in questo contesto originario, l'IA non era stata ancora oggetto di riflessione[20]. Ciò avviene solo

conclusioni degli Avvocati generali, tra le quali ci si limita a segnalare solo le più recenti: conclusioni dell'Avv. gen. Szpunar, del 15 luglio 2021, C-261/20, *Thelen Technopark*, par. 76; dell'Avv. gen. Pitruzzella, del 16 luglio 2020, C-372/19, *SABAM*, par. 26; dell'Avv. gen. Bot, del 3 settembre 2015, C-121/14, *Regno Unito* c. *Parlamento e Consiglio*, par. 71; dell'Avv. gen. Kokott, del 30 gennaio 2014, C-557/12, *Kone e a.*, par. 66; dell'Avv. gen. Wathelet, del 15 gennaio 2014, C-533/12 *Corsica Ferries France*, par. 27; dell'Avv. gen. Villalon, del 5 maggio 2010, C-515/08, *Santos Palhota e a.*, par. 51. In letteratura, invece, si veda L. Azoulai, *The Court of Justice and the Social Market Economy: The Emergence of an Ideal and the Conditions for its Realization*, in *CMLR*, 2008, p. 1335 ss.; G. Contaldi, *Il significato attuale dell'economia sociale di mercato nell'ordinamento dell'Unione europea*, in *OIDU*, 2018, p. 544 ss.; D. Damjanovic, *The EU Market Rules as Social Market Rules: Why the EU Can Be a Social Market Economy*, in *CMLR*, 2013, p. 1685 ss.; P. De Pasquale, *L'economia sociale di mercato nell'Unione europea*, in *SIE*, 2014, p. 265 ss.; C. E. O' Sullivan, *The EU Between Market State Ideals and Social Market Economy Objectives – Placing the Social Market Economy within the Union's Constitutional History*, in D. Ferri, F. Cortese (eds.), *The EU Social Market Economy and the Law: Theoretical Perspectives and Practical Challenges for the EU*, Abingdon e New York, 2019, p. 17 ss.; A. Predieri, *L'economia sociale di mercato nell'Europa di Maastricht*, in *DCI*, 1995, p. 531 ss.

[20] Per una prima ricostruzione dell'ingresso dell'IA nel contesto del MUD, si rinvia alle riflessioni di A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020.

nel 2017, con la revisione intermedia nella quale, per la prima volta, inizia a emergere chiaramente la necessità per l'Unione di intervenire anche in questo settore, in quel momento esplicitata soltanto con la previsione di investimenti e con l'obiettivo di facilitare la ricerca. In seguito, nel 2018, la Commissione adotta una prima comunicazione sull'IA[21], successivamente arricchita, nel 2020, dalla pubblicazione di un Libro bianco[22]. Da ultimo, nel 2021, è presentata una ulteriore comunicazione[23], in concomitanza della proposta di regolamento.

Ora, considerando la pubblicazione a piè sospinto dei summenzionati atti atipici, due ordini di riflessioni possono essere svolti.

In primo luogo, sembra emergere la volontà della Commissione di intraprendere la via legislativa per accreditare l'Unione come un *global standard setter* in materia di IA e, al tempo stesso, tentare di colmare il divario di sviluppo con i principali concorrenti a livello globale. Non è quindi una coincidenza che, accanto ai lavori preparatori della proposta di regolamento IA, si siano nel tempo affiancati una pletora di altri atti, afferenti materie solo apparentemente diverse, ma sempre legate dal *fil rouge* di rendere l'Unione maggiormente competitiva in ambiti nei quali sconta un forte *gap* di carattere tecnico. Ci si riferisce, in particolare, alla strategia sui *microchip*[24], ma anche agli sforzi profusi nel settore strategico della cibersicurezza. Ancora, notevole è il contributo della Commissione per quanto concerne la responsabilità da prodotto difettoso in materia di IA[25], lo spazio europeo

[21] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa, COM (2018) 237final, del 25 aprile 2018.

[22] Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM (2020) 65final, del 19 febbraio 2020.

[23] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Promuovere un approccio europeo all'intelligenza artificiale, COM (2021) 205final, del 21 aprile 2021.

[24] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una normativa sui *chip* per l'Europa, COM (2022) 45final, dell'8 febbraio 2022.

[25] Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale, COM (2022) 496final, del 28 settembre 2022. V. anche A. Castagnedi, *La grande corsa verso un modello di intelligenza artificiale affidabile: il Parlamento europeo propone un nuovo regime di responsabilità civile*, in *EJ*, 2021, p. 114 ss.

dei dati sanitari[26] e dei dati non personali[27]. Anche qui, lo si vedrà meglio nel prosieguo, è particolarmente avvertita la necessità di addivenire a un bilanciamento tra l'armonizzazione del mercato interno[28], evitando possibili frammentazioni nazionali che possano comprometterne il buon funzionamento, e il forte impatto sui diritti fondamentali.

In secondo luogo, si evince come questa incessante attività preparatoria, che si manifesta per lo più attraverso l'uso delle comunicazioni, debba necessariamente giungere a compimento con l'adozione di atti tipici di diritto derivato. In proposito, sembra potersi rinvenire una tendenza difficilmente controvertibile nel MUD nella misura in cui il regolamento, a causa delle sue caratteristiche, sia l'atto da preferire rispetto alla direttiva. Infatti, attraverso l'uso di quest'ultimo, l'Unione occupa un intero spazio legislativo, lasciando solo taluni – ben delineati quanto limitati – margini di manovra all'attività normativa statuale con ciò creando un *level playing field* dalle caratteristiche uniformi. Questo fenomeno se, da un lato, sembra ascriversi in prima battuta alle caratteristiche del regolamento, a ben vedere, è dovuto all'incisività della regolamentazione proposta, aspetto saliente soprattutto nel MUD.

Sembra, dunque, necessario fornire qualche dato qualitativo e quantitativo per provare a tracciare i caratteri essenziali di questa tendenza[29]. Innanzitutto, il regolamento generale sui dati personali[30] (RGDP) ha abrogato una direttiva. Ancora, sembra opportuno menzionare i due

[26] Proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM (2022) 197final, del 3 maggio 2022.

[27] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[28] Per il concetto di armonizzazione, sul quale si tornerà diffusamente *infra*, si richiama innanzitutto S. Weatherill, *Harmonization in the EU Internal Market*, in *Oxford Encyclopedia of EU Law*, Oxford, 2024, p. 1 ss. Sull'armonizzazione come processo di carattere anche costituzionale e istituzionale, si veda L. Azoulai, *The Complex Wave of Harmonization*, in D. Chalmers, A. Arnull (eds.), *The Oxford Handbook of European Union Law*, 2015, p. 589 ss.

[29] Per una efficace ricostruzione, G. Caggiano, *Il quadro normativo del mercato unico digitale*, in F. Rossi Dal Pozzo (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, *Fasciscolo speciale in EJ*, 2020, p. 13 ss.

[30] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

regolamenti sui mercati[31] e sui servizi digitali[32] ma anche il regolamento sugli utenti commerciali delle piattaforme digitali[33], il regolamento sui blocchi geografici[34], il regolamento sul *roaming*[35], il regolamento sulla cibersicurezza[36], il regolamento sulle locazioni brevi[37], sull'identità digitale[38] e sulla libertà dei media[39]. Una notevole eccezione si rinviene, invece, nella proposta di direttiva sui lavoratori delle piattaforme[40]. Vero è, però, che quest'ultima non presenta l'art. 114 TFUE come base giuri-

[31] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828.

[32] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

[33] Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

[34] Regolamento (UE) 2018/302 del Parlamento europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE.

[35] Regolamento (UE) 2022/612 del Parlamento europeo e del Consiglio, del 6 aprile 2022, relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

[36] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013. Particolarmente interessante è l'intersezione tra cibersicurezza, intelligenza artificiale e dispositivi medici; sul punto, E. Scalcon, *Cibersicurezza e dispositivi medici: la tutela della salute e della sicurezza dei pazienti dalle vulnerabilità informatiche nel Regolamento (UE) 2017/745 e nell'Artificial Intelligence Act*, in *BioLaw Journal – Rivista di biodiritto*, 2024, p. 183 ss.

[37] Regolamento (UE) 2024/1028 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, relativo alla raccolta e alla condivisione dei dati riguardanti i servizi di locazione di alloggi a breve termine e che modifica il regolamento (UE) 2018/1724.

[38] Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[39] Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE, COM (2022) 457final, del 16 settembre 2022.

[40] Proposta di direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, COM (2021) 762final, del 9 dicembre 2021.

dica, aspetto che accomuna invece gli atti sopra elencati e la direttiva sulla cibersicurezza[41].

Inoltre, proprio a causa della sovrabbondanza del ricorso ai regolamenti, pare opportuno interrogarsi anche sul coordinamento tra le loro disposizioni, soprattutto quelle aventi carattere squisitamente definitorio e che ne delimitano il campo di applicazione materiale. In realtà, al momento, la questione non sembra investire quello sull'IA per la semplice considerazione che esso è il primo a fornire una definizione di sistema di IA. Sarà la Commissione, in futuro, a dover garantire detto coordinamento, anche al fine di evitare incertezze interpretative e applicative da parte dei giudici, oltre che per assicurare la certezza del diritto agli operatori economici.

Quest'ultima preoccupazione trae, invero, origine dall'esperienza di altri regolamenti ove i profili di coordinamento, quantomeno per ciò che attiene alle definizioni normative, non sempre risultano compiutamente intellegibili, come quanto repentinamente avvenuto nel settore delle piattaforme digitali. Infatti, il punto di partenza è la nozione di servizio della società dell'informazione ai sensi dell'art. 1, par. 1, lett. *b*), dell'omonima direttiva[42] secondo il quale esso è qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Su di esso, è poi ricalcato il servizio di intermediazione *online* secondo l'art. 2, par. 2, del regolamento sugli utenti commerciali delle piattaforme digitali. Ancora, l'art. 2, par. 2, del regolamento sui mercati digitali si riferisce ai servizi di piattaforma di base includendovi i summenzionati servizi di intermediazione *online*. Infine, la proposta di direttiva sui lavoratori delle piattaforme utilizza la nozione di piattaforma di lavoro digitale richiamando, in parte, la definizione di servizio della società dell'informazione. In altre parole, la proliferazione dei regolamenti certamente contribuisce all'unitarietà o, se si preferisce, a evitare la potenziale frammentazione del MUD. Tuttavia, di converso, l'efficacia di detta scelta dipende anche, se non soprattutto, dall'armonico coordinamento con tutti gli altri atti presenti nel MUD.

[41] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[42] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

Vieppiù, la scelta del regolamento se, da un lato, ha il pregio di evitare l'intervento degli Stati membri – con i possibili inadempimenti che potrebbero derivare da una tardiva trasposizione di una direttiva – e la possibilità di invocarne l'effetto diretto anche nelle situazioni orizzontali[43], non elimina del tutto alcune potenziali incertezze applicative, sulle quali si ritornerà nel paragrafo seguente. Sul punto, infatti, appare emblematica la scelta di proporre due regolamenti in materia IA: il primo, quello qui in commento, per quanto riguarda i profili trasversali della materia, e il secondo, ancora in fase di adozione e già menzionato in precedenza, sulla responsabilità del produttore.

Come noto, inoltre, per il completamento del MUD, le comunicazioni e il regolamento IA insistono sull'immissione in commercio di sistemi che siano sicuri e che, essenzialmente, non comprimano ovvero non rischino di comprimere i diritti fondamentali protetti dalla Carta. In proposito, assumono particolare rilevanza i profili antidiscriminatori, come richiamati in molte disposizioni di diritto primario, segnatamente, gli articoli 9 e 18 TFUE accompagnati dall'art. 21 della Carta. Si pensi, infatti, al tema sempre più discusso della c.d. discriminazione algoritmica e al c.d. punteggio sociale, soprattutto per quanto concerne aspetti solo apparentemente neutri della vita quotidiana degli individui, come il luogo di residenza. Può, quest'ultimo, essere automaticamente considerato un parametro di solvibilità nella richiesta di mutuo laddove l'individuo risieda in una zona densamente popolata da etnie diverse? In questo senso, anche l'art. 12 TFUE e l'art. 38 della Carta, dedicati alla tutela dei consumatori, rappresentano un perimetro di sicurezza nel confronto di trattamenti interamente automatizzati e potenzialmente pregiudizievoli.

Su questi temi specifici, attinenti al bilanciamento tra diritti fondamentali e libertà economiche, si innestano altrettanti profili classici dell'ordinamento giuridico dell'Unione europea, quali quelli concernenti i principi di sussidiarietà e di proporzionalità, e l'utilizzo dell'art. 114 TFUE, in congiunzione con l'art. 16 TFUE, quali basi giuridiche del regolamento IA.

[43] Sul punto, si rinvia integralmente a F. COSTAMAGNA, *Diritti fondamentali e rapporti tra privati nell'ordinamento dell'Unione europea*, Torino, 2022.

3. *Basi giuridiche, armonizzazione, sussidiarietà, proporzionalità e diritti fondamentali: un facile bilanciamento?*

La tecnica legislativa usata per l'adozione del regolamento IA è consolidata e prevede un sapiente bilanciamento tra le esigenze del completamento del MUD e la tutela dei diritti fondamentali degli individui.

In prima battuta, il mercato interno è una materia di competenza concorrente secondo l'art. 4, par. 2, lett. *a*), TFUE. Di conseguenza, la scelta delle basi giuridiche è rigorosa. L'art. 114 TFUE è affiancato dall'art. 16 TFUE, entrambi prevedendo la procedura legislativa ordinaria. Sul punto appaiono anche superate le incertezze legislative, giurisprudenziali e dottrinarie che avevano contribuito a creare un ricco dibattito sugli intrecci tra la disciplina dei prodotti del tabacco e la tutela della salute[44].

Si è, dunque, in presenza di un facile bilanciamento tra esigenze del mercato e rispetto dei diritti fondamentali? E questo bilanciamento è stato correttamente perseguito tramite un atto di armonizzazione massima?

Ora, partendo dal presupposto che l'Unione abbia esercitato la propria competenza concorrente *ex* art. 4, par. 2, lett. *a*), TFUE in modo talvolta poco intellegibile[45], o meglio, cercando di adeguarsi alle contingenze del momento, sulla questione del bilanciamento tra mercato interno e diritti fondamentali nella fase legislativa possono essere svolti due ordini di considerazioni sulla tecnica legislativa del bilanciamento stesso e sul rispetto dei principi ad essa sottesi. Ciò necessariamente si interseca con l'armonizzazione massima[46] e, conseguentemente, con l'abbandono – quantomeno nel MUD – dell'armonizzazione minima[47]. Effettivamente, come è stato evidenziato nel paragrafo precedente, la scelta del regolamento quale atto *migliore* nel MUD sembra caratterizzare l'intera politica legislativa dell'Unione in *subiecta materia*.

Per quanto riguarda il primo ordine di considerazioni, esaminando la

[44] S. Weatherill, *The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law has become a "Drafting Guide"*, in *German Law Journal*, 2019, p. 827 ss.

[45] G. Davies, *The Competence to Create an Internal Market: Conceptual Poverty and Unbalanced Interests*, in S. Garben, I. Govaere (eds.), *The Division of Competences between the EU and the Member States*, cit., p. 74 ss.

[46] S. Weatherill, *The Fundamental Question of Minimum or Maximum Harmonisation*, S. Garben, I. Govaere (eds.), *The Internal Market 2.0*, Oxford-London, 2020, p. 261 ss.

[47] M. Dougan, *Minimum Harmonization and the Internal Market*, in *CMLR*, 2000, p. 853 ss.

giurisprudenza della Corte di giustizia, i precedenti relativi al bilanciamento tra libera circolazione e diritti fondamentali costituiscono uno dei punti di forza di un ordinamento che, seppur sprovvisto di una specifica competenza in materia, intenda, cionondimeno, proteggere i diritti fondamentali. A solo fine storico ricostruttivo, in un momento in cui la Carta non aveva ancora assunto carattere vincolante e rango primario, la Corte era già puntualmente intervenuta. Si pensi alla giurisprudenza *Omega*[48], dove i giudici di Lussemburgo dichiararono che la tutela della dignità umana può ergersi a esigenza imperativa qualora si tratti di restringere la libera prestazione dei servizi. Ancora, con la sentenza *Schmidberger*[49] la Corte ha bilanciato le restrizioni alla libera circolazione delle merci con la libera manifestazione del pensiero. Più di recente, e con specifico riferimento alla tutela dei dati personali, la Corte ha annullato la decisione della Commissione relativa al c.d. sistema *Safe Harbour*[50]. I precedenti, dunque, militano in favore di un approccio rigoroso e condivisibile, volto a garantire la tutela dei diritti fondamentali. Certo, in futuro il bilanciamento avverrà tenendo in considerazione la *vis espansiva* del MUD ma gli approdi teorici cui si è pervenuti appaiono sufficientemente solidi da reggere il confronto con la digitalizzazione e l'avvento delle nuove tecnologie come l'IA.

Il secondo ordine di considerazioni attiene ai principi di sussidiarietà e di proporzionalità, i quali, in verità, non sembrano porre particolari interrogativi. Data la dimensione, la scala e gli effetti previsti non sono state sollevate perplessità sul loro rispetto[51]. Esso è, infatti, assodato e, ormai, *in re ipsa*, con la Commissione che si limita a inserire alcune clausole di stile nei considerando dell'atto. Né, come noto, la Corte si è spinta a scrutinarne il rispetto, riconoscendo l'ampio margine di discrezionalità conferito al legislatore una volta che quest'ultimo abbia deciso di procedere. Inoltre, non si registrano incertezze da parte dei Parlamenti nazionali che, chiamati a esprimere il loro parere, non hanno sollevato obiezioni[52].

[48] Corte giust. 14 ottobre 2004, C-36/02.

[49] Corte giust. 12 giugno 2003, C-112/00.

[50] Corte giust. 6 ottobre 2015, C-362/14, *Schrems*.

[51] È stato efficacemente sottolineato in letteratura come ormai il rispetto di tali principi sia per lo più affidato alla presenza di mere clausole di stile nei considerando degli atti legislativi. P. De Pasquale, *Sharing is caring: i primi trent'anni del principio di sussidiarietà nell'Unione europea*, in *DUE*, 2021, p. 429 ss.

[52] Gli Stati membri i cui Parlamenti hanno espresso il parere concernente il rispetto dei principi di sussidiarietà e proporzionalità sono i seguenti: Austria, Belgio, Croazia, Cechia, Danimarca, Estonia, Francia, Germania, Italia, Lituania, Malta, Paesi Bassi, Polonia, Romania, Slovacchia, Slovenia, Spagna. I dati sono accessibili al *link* www.ipex.eu/IPEXL-WEB/

In concreto, le suesposte riflessioni trovano un aggancio tanto nei considerando quanto nelle disposizioni del regolamento IA. Da un lato, i primi si riferiscono al fatto che taluni Stati membri stiano già ipotizzando l'adozione di norme nazionali volte a disciplinare l'IA, con ciò potendo comportare sia una frammentazione del mercato sia una riduzione della certezza del diritto. Di conseguenza, la garanzia di sicurezza e tutela dei diritti fondamentali potrebbe essere compromessa. Per quanto attiene, invece, alla scelta dell'atto si legge espressamente che «le disposizioni del regolamento non sono *eccessivamente* [corsivo aggiunto] prescrittive e lasciano spazio a diversi livelli di azione da parte degli Stati membri in relazione ad aspetti che non pregiudicano il conseguimento degli obiettivi dell'iniziativa, in particolare l'organizzazione interna del sistema di vigilanza del mercato e l'adozione di misure destinate a promuovere l'innovazione[53]». In particolare, il Titolo VI (*Governance*) e il Titolo VIII (Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato) confermano la volontà del legislatore di lasciare taluni ben determinati spazi di manovra agli Stati. Posto che, a norma dell'art. 59 del regolamento, «ciascuno Stato membro istituisce o designa autorità nazionali competenti al fine di garantire l'applicazione e l'attuazione» e che, secondo il successivo par. 4, gli Stati membri «garantiscono che le autorità nazionali competenti dispongano di risorse finanziarie e umane adeguate per svolgere i loro compiti» rimane il dubbio di una potenziale frammentazione a livello nazionale. Sembra, del resto, non potersi escludere la possibilità che alcune di tali autorità non siano adeguatamente equipaggiate, tanto sotto il profilo economico quanto quello delle competenze tecniche. Da un angolo differente emerge, poi, l'obbligo per gli Stati membri di agevolarne il coordinamento secondo l'art. 63, par. 7. Anche in questo contesto, è di cruciale importanza la verifica dell'esercizio da parte degli Stati membri della discrezionalità loro attribuita.

Un altro elemento di flessibilità si rinviene, poi, nell'uso del linguaggio. L'art. 47, par. 1, si riferisce a motivi «eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente e dei principali beni industriali e infrastrutturali», elementi che saranno valutati dagli organismi di vigilanza. Ancora, l'art. 10, par. 2, lett. *f*), indica «potenziali distorsioni» mentre l'art. 13 menziona un «funzionamento dei […] sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente». Questi elementi di carat-

document/COM-2021-0206.

[53] COM (2021) 206final, cit., p. 8.

tere testuale si contraddistinguono per un livello di indeterminatezza che pare contrastare con l'obiettivo dichiarato di creare un *level playing field* per i produttori di sistemi di IA.

Purtuttavia, complessivamente inteso, l'approccio del legislatore, dunque, pare voler superare la rigida distinzione tra armonizzazione minima e massima in favore di un approccio maggiormente pragmatico, probabilmente dettato dall'ambito specifico oggetto di intervento normativo.

In altre parole, con il regolamento IA l'Unione ha inteso armonizzare il settore dell'IA precludendo agli Stati membri spazi di manovra che, altrimenti, avrebbero potuto compromettere un approccio unitario ai profili delle nuove tecnologie che impattano sui diritti dei singoli. Alcune criticità, come si è visto, permangono rispetto alla formazione dei comitati di controllo che saranno composti da soggetti aventi carattere *nazionale*[54], con ciò, quantomeno astrattamente, minando la possibilità di avere una visione genuinamente *comunitaria*, dei profili di valutazione del rischio. Peraltro, questa forma di decentramento pare non collimare esattamente con la creazione, all'interno della Direzione generale *Communication Networks, Content and Technology* della Commissione dell'Ufficio europeo per l'intelligenza artificiale[55].

4. *Osservazioni conclusive*

Una valutazione complessiva del regolamento IA è ancora prematura in assenza sia di una prassi applicativa – tanto a livello nazionale quanto a livello della Commissione – sia di giurisprudenza della Corte di giustizia. Cionondimeno, l'interesse che la materia ha attirato dimostra, da un lato, la preoccupazione dovuta a potenziali violazioni dei diritti fondamentali degli individui salvaguardati dalla Carta; dall'altro lato, la sempre viva curiosità verso le tecniche legislative impiegate per normare fenomeni digitali e tecnologici che, per loro stessa natura, faticano a essere incapsulati all'interno di rigide categorie giuridiche. Sotto entrambi questi profili, l'IA non costitu-

[54] Sul punto si rinvia a S. Villani, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in questo *fascicolo speciale*.

[55] Decisione della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale, C/2024/390, del 14 febbraio 2024. Sui poteri della Commissione in esecuzione del regolamento IA, si rinvia a F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in questo *fascicolo speciale*.

isce un'eccezione, basti pensare alle ulteriori sfide regolatorie poste, a titolo di esempio, dalle c.d. criptovalute, dalle identità digitali e dalla *blockchain*. L'attività legislativa è, quindi, incessante, come si è visto nel settore delle piattaforme digitali. Semmai, occorrerebbe verificare se, ed eventualmente in che misura, il diritto – tanto più quello derivante da un ordinamento giuridico di *nuovo genere* –, l'attività legislativa, *rectius*, le procedure legislative ordinarie basate sull'art. 114 TFUE e, potenzialmente, anche sull'art. 16 TFUE, siano in grado di concludersi entro tempi ragionevoli, laddove la *ragionevolezza* è necessariamente dettata dalla velocità delle nuove tecnologie.

Effettivamente, pare comprendersi che il regolamento IA rappresenti solo il primo degli atti giuridici in materia poiché, come anticipato, è ancora in corso la procedura legislativa ordinaria che porterà all'adozione di un altro regolamento – anch'esso avente per base giuridica l'art. 114 TFUE – sulla responsabilità da prodotto difettoso. Su questo profilo specifico, sembra difficile esporre un'opinione definitiva. Da un lato, il regolamento IA è già di per sé particolarmente complesso e aggiungere profili delicati come quelli attinenti la responsabilità avrebbe richiesto uno sforzo ulteriore con il rischio di dilatarne eccessivamente l'adozione e, di conseguenza, lasciare l'IA in un limbo giuridico. Dall'altro lato, con la previsione di un regolamento a sé stante, il coordinamento tra i due atti sarà demandato non solo e non tanto alle loro stesse norme ma, in caso di controversie, ai giudici nazionali ed eventualmente, tramite rinvii pregiudiziali, alla Corte. Dunque, anche questo elemento di riflessione non trova una conclusione esauriente, persuadendo l'interprete a sospendere le proprie valutazioni.

Ciò che rimane di certo – per l'interprete, per i produttori e per i consumatori – è, in ultima analisi, l'obiettivo del regolamento IA, ossia, lo si ribadisce, la messa in commercio di sistemi di IA sicuri, basati su un approccio complessivamente inteso alla prevenzione e alla gestione del rischio nella sua più ampia accezione[56]. Sotto questo angolo visuale, a dispetto dell'intrinseca novità dell'oggetto da regolare, la tecnica legislativa è consolidata e affonda le proprie radici già negli anni '90. Si pensi, semplicemente, al regolamento sulla sicurezza alimentare

[56] Per ragioni di spazio ed economia espositiva, il presente contributo non può esaminare gli aspetti generali e specifici attinenti, da un lato, alla gestione del rischio e, dall'altro, alle specifiche casistiche di rischio alto, medio e basso. I singoli profili sono stati, invece, esaminati in letteratura. H. Fraser, J. M. Bello y Villarin, *Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough*, in *European Journal of Risk Regulation*, 2023, p. 1 ss.; P. Loi, *Il rischio proporzionato nella proposta di regolamento sull'IA e i suoi effetti nel rapporto di lavoro*, in *federalismi.it*, 2023, p. 239 ss.; J. Schuett, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023, p. 1 ss.

che ha istituito l'EFSA[57]. Esso richiama sia le esigenze di libera circolazione delle merci, ossia, nel caso di specie, degli alimenti per uso umano, sia la necessità che questi siano sicuri; del resto, l'atto era basato sul previgente art. 95 TCE, oltre che sugli articoli 37, 133 e 152, par. 4, lett. *b*), TCE.

L'unico modo per addivenire a un idoneo bilanciamento tra esigenze di completamento e buon funzionamento del mercato interno e *altri* interessi idonei a essere tutelati – che siano i diritti fondamentali o meno – è per il tramite dell'art. 114 TFUE, accompagnato di volta in volta da altre basi giuridiche, sempre, però, nel rispetto di una unica procedura legislativa. In questo contesto, se ne può rammentare l'utilizzo anche nella direttiva sui c.d. *whistleblower*[58] nella misura in cui, accanto ad esso, ne sono richiamate altre dieci.

Alla luce delle suesposte considerazioni, l'accorto bilanciamento tra mercato e diritti presente nel regolamento IA potrebbe, conseguentemente, inquadrarsi nella *formula* dell'economia di mercato fortemente competitiva, secondo l'art. 3, par. 3, TUE, la quale – non è una coincidenza – si attaglia proprio al completamento del mercato interno e, *in extenso*, del MUD.

Da un punto vista sistemico, è esattamente in questo profilo che si rinviene la bontà dell'opera del legislatore. Se, infatti, a lungo l'Unione è parsa preoccuparsi maggiormente di aumentare la propria competitività sui mercati, trascurando gli aspetti più squisitamente, sociali o, se si preferisce, legati all'innalzamento della tutela dei diritti, il regolamento IA ne fa la propria *raison d'être*. Quanto ciò si realizzerà in modo tangibile nella vita quotidiana degli individui dovrà essere oggetto di studi negli anni a venire.

La portata del cambio di paradigma, se non addirittura di linguaggio[59], imposto dall'IA, è destinata a riflettersi anche nelle attività interistituzionali, come evidenziato dalla Dichiarazione sui diritti e principi digitali per il decennio digitale[60].

[57] Regolamento (CE) 178/2002 del Parlamento europeo e del Consiglio, del 28 gennaio 2002, che stabilisce i principi e i requisiti generali della legislazione alimentare, istituisce l'Autorità europea per la sicurezza alimentare e fissa procedure nel campo della sicurezza alimentare

[58] Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione. Accanto all'art. 114 TFUE, l'atto è basato sulle seguenti norme: articolo 16, l'articolo 43, paragrafo 2, l'articolo 50, l'articolo 53, paragrafo 1, gli articoli 91, 100 e 114, l'articolo 168, paragrafo 4, l'articolo 169, l'articolo 192, paragrafo 1, e l'articolo 325, paragrafo 4 TFUE.

[59] A. D'Aloia, *Ripensare il diritto nel tempo dell'intelligenza artificiale*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione*, Bologna, 2022, p. 79 ss.

[60] Dichiarazioni comuni, Parlamento europeo, Consiglio, Commissione europea, Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, 2023/C 23/01. Per

Per giunta, se finora la letteratura si è concentrata su come il diritto insegua l'innovazione tecnologica – o su come sia necessario aggiornare il concetto di mercato interno[61] – e come la regolamentazione debba tutelare i diritti fondamentali[62], iniziano ad affacciarsi anche nuovi studi. Ad esempio, è stato solo parzialmente esplorato il tema dell'impatto dell'IA sul cambiamento climatico[63] e, più in generale, sulla sostenibilità ambientale. Ancora, l'autonomia dell'individuo, nella sua capacità di negoziare in quanto consumatore, potrebbe essere compressa[64]. Inoltre, i profili del coordinamento non attengono solo al regolamento IA e alla responsabilità del produttore ma anche, quando le imprese avranno raggiunto una posizione particolarmente *grande* nel mercato interno, potranno essere designate dalla Commissione come *gatekeeper* secondo il regolamento sui mercati digitali, con ciò essendo soggette a obblighi aggiuntivi[65]. Infine, una specifica applicazione cumulativa si prospetta anche con il RGDP, soprattutto per quanto attiene l'individuazione del titolare del trattamento dei dati[66].

Come autorevolmente sostenuto, l'Unione, quindi si muove in una dimensione in cui il proprio mercato interno[67], da ultimo evolutosi nel MUD, possa iniziare a fungere da collettore di rinnovate esigenze, cui la risposta istituzionale deve essere la garanzia per gli individui di beni e servizi tanto sicuri quanto avanzati.

Abstract (ita)

le primi analisi si rinvia a L. Cianci, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?*, in *DPCE*, 2022, p. 381 ss.; P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *DUE*, 2022, p. 163 ss.

[61] I. Lianos, *Updating the EU Internal Market Concept*, in F. Amtenbrink, G. Davies, D. Kochenov, J. Lindeboom (eds.), *op. cit.*, p. 495 ss.

[62] V. anche V. Kosta, *Fundamental Rights in EU Internal Market Legislation*, London, New York, 2018.

[63] F. Cortez, *Artificial Intelligence, Climate Change and Innovative Democratic Governance*, in *European Journal of Risk Regulation*, 2023, p. 484 ss.

[64] S. Fassiaux, *Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach*, in *European Journal of Risk Regulation*, 2023, p. 710 ss.

[65] P. Hacker, J. Cordes, J. Rochon, *Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond*, in *European Journal of Risk Regulation*, 2023, p. 49 ss.; P. Hacker, *Sustainable AI Regulation*, in *CMLR*, 2024, p. 345 ss.

[66] G. Contaldi, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea sui mercati digitali*, Bari, 2021, p. 207 ss.

[67] E. Letta, *Much more than a Market. Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for all EU Citizens*, 2024, disponibile *online:* www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf.

Il presente contributo intende contestualizzare il regolamento sull'intelligenza artificiale (IA) nel più ampio quadro legislativo relativo al completamento del mercato unico digitale. In particolare, esso si presta a una duplice analisi: da un lato, presenta indubbi profili di carattere costituzionale, concernenti, nello specifico, il bilanciamento tra tutela dei diritti degli individui e immissione sul mercato interno di dispositivi di IA comportanti dei rischi; dall'altro lato, il regolamento è basato anche sull'art. 114 TFUE, norma cardine dell'architettura del mercato interno. Il presente contributo, quindi, si interroga sulla capacità del legislatore di addivenire a una sintesi tra due esigenze solo apparentemente contrapposte, le quali, in verità, esprimono la propria *raison d'être* nella locuzione di «economia sociale di mercato fortemente competitiva» secondo l'art. 3, par. 3, TUE.

Abstract (eng)

This paper wishes to position the artificial intelligence (AI) Regulation within the wider legislative framework related to the internal market's completion. In particular, the Regulation can be analysed from a twofold perspective. On the one hand, it undoubtedly showcases certain constitutional features, related to the balance between individuals' rights protection and the market of dangerous AI systems. On the other hand, Article 114 TFUE – the norm upon which the internal market architecture is grounded – is the Regulation's legal basis too. This paper, hence, questions the legislator's ability to find a balance between two only apparently competing interests which, indeed, features their *raison d'être* in the expression «highly competitive social market economy» according to Article 3 (3) TEU.

IL RUOLO DELLE NORME ARMONIZZATE NELL'ATTUAZIONE DEL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE

Annalisa Volpato*

SOMMARIO: 1. Introduzione. – 2. L'uso delle norme armonizzate nel diritto dell'Unione e le sue criticità. – 3. Il rinvio alle norme armonizzate nell'art. 40 AIA e la sua attuazione: dalla proposta al testo del regolamento. – 3.1. La richiesta di normazione e la questione dei diritti fondamentali. – 4. Considerazioni conclusive.

1. *Introduzione*

L'adozione del regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (di seguito "AIA", dall'inglese *Artificial Intelligence Act*) costituisce una tappa miliare nella regolazione delle nuove tecnologie digitali nell'Unione europea ("UE"). Con l'approvazione del Parlamento europeo il 13 marzo 2024[1], e del Consiglio dell'Unione europea il 21 maggio 2024[2], l'UE diviene uno dei primi ordinamenti giuridici a dotarsi di un quadro normativo in materia[3]. Nella specie l'AIA si caratterizza per gli obiettivi che persegue, ovvero la tutela della sicurezza e dei diritti fondamentali degli individui sanciti dalla Carta dei diritti fondamentali dell'Unione europea (la

* Ricercatrice in diritto dell'Unione europea presso l'Università degli Studi di Padova. Il presente contributo risulta dalle attività di ricerca del progetto PRoTecTS (Protecting Individuals in the Private Regulation of Digital Technologies) finanziato dall'Unione Europea – NextGenerationEU e dal programma STARS@UNIPD.

[1] Risoluzione legislativa del Parlamento europeo, del 13 marzo 2024, sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

[2] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (legge sull'intelligenza artificiale).

[3] Nonostante la proposta della Commissione europea sia stata la prima iniziativa legislativa in questo senso, l'approvazione definitiva dell'AIA è posteriore all'adozione del Colorado AI Act (CAIA) (SB-205), datato 17 maggio 2024. Pur avendo una portata più limitata, v. anche US Blueprint for an AI Bill of Rights (2022) e Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (2023); e "Misure provvisorie per la gestione dei servizi di intelligenza artificiale generativa" della Repubblica Popolare Cinese (2023).

"Carta"), nonché dei valori fondanti l'ordinamento quali la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro il possibile impatto negativo derivante dallo sviluppo e dall'uso di sistemi di intelligenza artificiale ("IA").

L'AIA presenta un forte carattere innovativo non soltanto per l'oggetto e per la comprensività delle sue norme, che si applicano a tutti i sistemi di IA immessi nel mercato e utilizzati nell'UE, ma anche per il particolare approccio basato sul rischio (*risk-based approach*)[4] che distingue i sistemi di IA in categorie, alle quali corrispondono diversi regimi regolatori progressivamente più stringenti. Sulla base dei loro effetti sulla salute, sulla sicurezza, o sui diritti fondamentali dell'individuo, il regolamento identifica quattro categorie di rischio: rischio inaccettabile, rischio alto, rischio limitato, e rischio minimo[5]. Mentre le pratiche IA inaccettabili sono semplicemente vietate nell'Unione[6], per i sistemi IA ad alto rischio l'AIA stabilisce una serie di obblighi di trasparenza, documentazione e vigilanza la cui attuazione attraverso disposizioni precise e di dettaglio richiederà specifiche competenze tecnologiche ed informatiche. A questo fine, la normazione tecnica «dovrebbe svolgere un ruolo fondamentale nel fornire soluzioni tecniche ai fornitori per garantire la conformità» all'AIA[7]. Questa attività è tipicamente affidata a organizzazioni private, composte da esperti del settore e attive a livello europeo. Sotto questo aspetto, l'AIA si pone in un solco ben tracciato, facendo ricorso ad una tecnica legislativa di rinvio – il cosiddetto "Nuovo Approccio" – che ha segnato la realizzazione del mercato interno sin dagli anni Ottanta e sulla quale la dottrina ha sollevato numerose critiche. È proprio in relazione a tale scelta normativa e alle sue specifiche implicazioni per un settore tanto delicato come quello dell'IA che sembra opportuno qui soffermarsi.

Il presente contributo ricostruisce brevemente l'evoluzione della normazione tecnica e della tecnica legislativa di rinvio alle norme armonizzate in diritto dell'Unione, dando conto dei recenti sviluppi giurisprudenziali e dei profili problematici che sono emersi (§2). Successivamente, analizza in dettaglio il ruolo delle norme tecniche all'interno del quadro normativo dell'AIA e offre alcune riflessioni preliminari sulle implicazioni giuridiche

[4] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, n. 2, 2022.

[5] A seguito delle negoziazioni in trilogo, a queste categorie si aggiunge una disciplina a parte per i modelli di IA per finalità generali, v. art. 51 AIA.

[6] Art. 5 AIA.

[7] Considerando n. 121 AIA.

del loro uso nell'ambito della tutela dei diritti fondamentali e della partecipazione democratica alla regolazione delle tecnologie digitali (§3), prima di presentare delle considerazioni conclusive (§4).

2. *L'uso delle norme armonizzate nel diritto dell'Unione e le sue criticità*

L'uso delle norme tecniche al fine di completare ed attuare atti vincolanti dell'UE è una tecnica legislativa consolidata in diritto dell'Unione[8]. Sin dal 1985, il legislatore europeo ha fatto affidamento su questi strumenti non vincolanti, di applicazione volontaria e di provenienza privata, per la definizione degli aspetti più tecnici e complessi della regolazione dei prodotti industriali e, successivamente, dei servizi nel mercato interno[9]. La tecnica legislativa del Nuovo Approccio (ora chiamata anche "New Legislative Framework") consiste nell'inserire negli atti legislativi soltanto i requisiti essenziali di interesse generale (quali i livelli di salute e sicurezza dei prodotti) e rimandare la definizione dettagliata delle regole tecniche ad una delle tre organizzazioni europee di normazione ("OEN" o "ESOs", dall'inglese *European standardisation organisations*), ovvero CEN, CENELEC ed ETSI[10]. In particolare, a seguito dell'adozione di un regolamento o una direttiva di armonizzazione, la Commissione europea invia una richiesta ad una delle OEN di elaborare un documento che definisca i requisiti tecnici (quali la composizione, le dimensioni, le caratteristiche di qualità ecc.) che devono essere soddisfatti da un prodotto, un processo, un servizio o un sistema. Questa richiesta, in passato chiamata più esplicitamente *mandato*, contiene ulteriori indicazioni e concorre a definire, assieme all'atto legislativo, i margini entro cui l'attività di normazione da parte delle OEN deve avvenire[11]. Le norme tecniche sono

[8] V. *inter alia* M. Eliantonio, C. Cauffman (eds.), *The Legitimacy of Standardization as a Regulatory Technique A Cross-disciplinary and Multi-level Analysis*, Cheltenham, 2020.

[9] Libro Bianco della Commissione per il Consiglio europeo, Il completamento del mercato interno, Milano, 28-29 giugno 1985; risoluzione del Consiglio, del 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione; risoluzione del Consiglio, del 21 dicembre 1989, concernente un approccio globale in materia di valutazione della conformità.

[10] Il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto Europeo per le norme di Telecomunicazioni (ETSI) sono le tre organizzazioni riconosciute nell'Allegato I del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea.

[11] Le OEN sono consultate prima dell'adozione della richiesta, la quale può essere da queste negoziata e anche formalmente rifiutata. A seguito dell'adozione del regolamento

quindi elaborate da queste organizzazioni, composte da rappresentanti degli organismi di normazione nazionali – a loro volta composti da soggetti che volontariamente partecipano al processo, generalmente esperti provenienti dalle imprese del settore industriale soggetto a regolazione – e inviati alla Commissione europea. Queste norme, adottate sulla base di una richiesta della Commissione per l'attuazione di un atto di armonizzazione europeo, sono definite «norme armonizzate»[12]. Se la Commissione ritiene che la norma tecnica sia conforme alla richiesta e all'atto legislativo, pubblica il suo riferimento nella Gazzetta ufficiale dell'Unione europea[13]. Sino al 2018 la pubblicazione del riferimento prendeva la forma di una comunicazione della Commissione[14], mentre ora avviene in forma di decisione d'esecuzione[15], non sottoposta a procedura di comitato[16]. In questo modo, tramite il combinato disposto dell'atto legislativo, della richiesta della Commissione e del suo successivo *endorsement* attraverso la pubblicazione del riferimento in Gazzetta ufficiale, la norma armonizzata entra nell'ordinamento giuridico dell'Unione in quanto tale, senza essere formalmente trasposta in alcun atto tipico dell'Unione.

La pubblicazione conferisce una presunzione di conformità alle relative disposizioni legislative per i prodotti che rispettano la norma armoniz-

1025/2012, cit., essa prende la forma di una decisione di esecuzione, sottoposta a procedura di comitato d'esame. V. art. 10 comma 2, in combinato disposto con l'art. 22 comma 3 del regolamento 1025/2012, che fa rinvio all'art. 5 del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione.

[12] Art. 2 par. 1 (c) del regolamento 1025/2012. V. anche Commissione europea, The "Blue Guide" on the implementation of EU products rules, 2016, punto 4.1.2.2.

[13] La pubblicazione contiene soltanto il codice di riferimento, non il testo della norma armonizzata. Il testo è coperto da copyright e le OEN ne permettono la fruizione a pagamento. V. B. Lundqvist, *European Harmonised Standards as 'Part of EU Law': The Implications of the James Elliott Case for Copyright Protection and, Possibly, for EU Competition Law*, in *Legal Issues of Economic Integration*, 2017, pp. 421-436.

[14] Era infatti pubblicato nella serie C della Gazzetta Ufficiale dell'Unione europea.

[15] Pubblicata nella serie L della Gazzetta Ufficiale dell'Unione europea. Sulle conseguenze di questo cambio di prassi, sia consentito rimandare a A. Volpato, *The Legal Effects of Harmonised Standards in EU Law: From Hard to Soft Law, and Back?*, in P. L. Láncos, N. Xanthoulis, L. Arroyo Jiménez (eds.), *The Legal Effects of EU Soft Law*, Cheltenham, 2023, pp. 193-212.

[16] Essa è però preceduta dalla consultazione dei c.d. "HAS consultants" (*Harmonised Standards consultants)*, ovvero soggetti privati legati alla Commissione europea da contratto di servizio. Dal 1° agosto 2022, il contratto di servizio è stato aggiudicato dall'azienda di consulenza Ernst & Young Global Limited.

zata, che potranno quindi essere commercializzati in tutto il territorio dell'UE senza ostacoli[17]. Le norme armonizzate elaborate dalle OEN sono formalmente non vincolanti poiché un operatore economico può sempre provare la conformità dei propri prodotti alla legislazione europea in maniera alternativa, fornendo prova della sicurezza dei propri prodotti attraverso test e certificati specificatamente ideati. Tuttavia, la presunzione di conformità stabilita dall'adeguamento della norma armonizzata ha rilevanti effetti giuridici e pratici per gli operatori economici, soprattutto quando è legata a meccanismi di certificazione[18]. Come dimostrato in dottrina, alla luce del contesto legislativo ed economico nel quale questi organismi operano, e della pratica dei mercati, è in realtà molto difficile e costoso provare la conformità di un prodotto alla legislazione europea in maniera diversa da quella prevista dalla norma armonizzata rilevante[19]. La giurisprudenza della Corte di giustizia ha riconosciuto che, in alcuni casi, queste norme volontarie devono considerarsi *de facto* vincolanti[20].

Complessivamente, si può ritenere che il coinvolgimento delle OEN nella regolazione europea abbia dato vita ad una solida *partnership* pubblico-privata che ha dato un'importante spinta alla realizzazione del mercato interno[21]. In quanto tale, esso rappresenta un esempio virtuoso di "co-regolazione", come metodo regolatorio partecipativo auspicato nell'accordo interistituzionale "Legiferare meglio"[22]. Tuttavia, il ruolo di questi organismi

[17] I diversi passaggi sono ora disciplinati dal regolamento 1025/2012. V. anche la recente modifica da parte del regolamento (UE) 2022/2480 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, recante modifica del regolamento (UE) n. 1025/2012 per quanto riguarda le decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti della normazione europea.

[18] V. decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti; regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che fissa le norme in materia di accreditamento.

[19] V. *inter alia* M. Eliantonio, C. Cauffman (eds.), *op. cit.*; H. Schepel, *The Constitution of Private Governance. Product Standards in the Regulation of Integrating Markets*, Oxford, 2005; J. Pelkmans, *The New Approach to Technical Harmonisation and Standardization*, in *Journal of Common Market Studies*, 1987, p. 249 ss.

[20] V. Tribunale 26 gennaio 2017, T-474/15, *Global Garden*, punto 67; Corte giust. 12 luglio 2012, C-171/11, *Fra.bo*. V. anche Corte giust. 31 marzo 2011, C-367/10 P, *EMC*.

[21] Comunicazione della Commissione europea, Norme armonizzate – Migliorare la trasparenza e la certezza del diritto per un mercato unico pienamente funzionante.

[22] Parlamento europeo, Consiglio dell'Unione europea e Commissione europea, Accordo interistituzionale "Legiferare meglio", del 13 aprile 2016. V. anche CEN-CENELEC, Guide 30, 1° ed., June 2015.

privati nella regolazione pubblica del mercato interno è apparso sin da subito problematico sotto il profilo democratico. In particolare, alcuni autori hanno rilevato come questo possa costituire una forma di delega di poteri ad organismi privati che è difficilmente compatibile con gli stretti limiti posti dalla giurisprudenza della Corte di giustizia, sollevando dubbi riguardo alla legittimità della prassi anche in relazione al difetto di *accountability* degli attori coinvolti[23]. Altri autori si sono concentrati sulle specifiche violazioni in materia di diritto della concorrenza e della tutela della proprietà intellettuale che questo fenomeno può favorire[24]. Infine, forti critiche sono state sollevate in relazione alla mancanza di trasparenza, partecipazione e accessibilità delle norme tecniche, la cui elaborazione è nelle mani di aziende private (spesso grandi aziende poiché soltanto queste hanno le risorse per partecipare ai lavori in maniera sistematica) senza garanzie procedurali o sostanziali per assicurare un'adeguata considerazione dell'interesse pubblico nel contenuto delle norme tecniche[25].

Queste preoccupazioni sono state fatte progressivamente proprie dalle istituzioni europee[26] ed hanno portato all'adozione del regolamento 1025/2012, che stabilisce il quadro giuridico generale per la cooperazione con le OEN e per l'elaborazione di norme armonizzate a fini regolatori. In particolare, esso contiene il diritto per il Parlamento europeo e gli Stati membri di sollevare obiezioni alla pubblicazione di un riferimento ad una norma armonizzata in Gazzetta ufficiale[27], nonché un meccanismo di finanziamento e di agevolazione della partecipazione di associazioni rappresentative degli

[23] C. Joerges, H. Schepel, E. Vos, *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the New Approach*, Badia Fiesolana, 1999; H. Schepel, *op. cit*.

[24] P. Arhel, *Comportements anticoncurrentiels dans le cadre de la normalisation*, in *Petites affiches*, n. 147, 2010, p. 4 ss.; F. Lévêque, *La normalisation et le droit de la concurrence face au hold-up*, in *Revue Lamy de la concurrence*, 2007, p. 170 ss.; B. Lundqvist, *European Harmonised Standards as 'Part of EU Law': The Implications of the James Elliott Case for Copyright Protection and, Possibly, for EU Competition Law*, in *Legal Issues of Economic Integration*, 2017, p. 421 ss.

[25] M. Eliantonio, M. Medzmariashvili, *Hybridity Under Scrutiny: How European Standardization Shakes the Foundations of EU Constitutional and Internal Market Law*, in *Legal Issues of Economic Integration*, n. 4, 2017.

[26] Risoluzione del Consiglio, del 18 giugno 1992, sulla funzione della normalizzazione europea nell'economia europea; Report on the report from the Commission to the Council and the European Parliament – "Efficiency and Accountability in European Standardisation under the New Approach", 1998.

[27] Regolamento 1025/2012, cit., art. 11.

interessi dei consumatori, dei lavoratori, dell'ambiente e delle PMI nei lavori delle OEN[28]. Benché questo abbia comportato un miglioramento della trasparenza e dell'inclusività della normazione tecnica europea, l'effettiva partecipazione da parte di queste associazioni rimane in realtà limitata per lo squilibrio di risorse economiche, di competenze tecniche e di riconoscimento formale tra queste e le aziende private che compongono storicamente le OEN[29].

Nel corso di questi anni, anche l'approccio della Corte di giustizia ha subito un'evoluzione. Se inizialmente le norme armonizzate non erano considerate rilevanti per la sfera giuridica in quanto private e non vincolanti, nella sentenza *James Elliott Construction* del 2016 la Corte ha ritenuto che esse debbano essere considerate parte integrante del diritto dell'UE, stabilendo la propria competenza ad interpretare il testo delle norme armonizzate ai sensi dell'art. 267 TFUE[30]. Questo perché la norma armonizzata costituisce «una misura di attuazione necessaria» della legislazione europea[31], che dunque assolve ad una funzione paragonabile a quella di un atto di esecuzione[32]. La giurisprudenza successiva della Corte ha confermato questo approccio, pur con qualche oscillazione[33]. Se infatti una recente sentenza ha fatto discendere dall'applicazione del principio di Stato di diritto la necessità che le norme armonizzate siano gratuitamente accessibili al pubblico[34], questo principio non è stato sinora valorizzato al punto di ammettere la possibilità di un ricorso giurisdizionale diretto avverso una norma armonizzata ai sensi dell'art. 263 TFUE[35]. Quel che è certo, tuttavia, è che il valore giuridico delle

[28] *Ibidem*, art. 5.

[29] Basti ricordare qui che queste associazioni non godono di diritto di voto nell'adozione delle norme armonizzate in CEN e CENELEC. Per un'analisi più dettagliata, sia consentito rimandare a M. Eliantonio, A. Volpato, *The European System Of Harmonised Standards. Legal Opinion for ECOS*, in *SSRN*, 2022.

[30] Corte giust. 27 ottobre 2016, C-613/14, punto 40. Su quella sentenza, sia consentito rimandare a A. Volpato, *The harmonized standards before the ECJ: James Elliott Construction*, in *CMLR*, n. 2, 2017, p. 591 ss.

[31] *James Elliott Construction*, sopra citata, punto 43.

[32] C. Tovo, *Judicial review of harmonized standards: Changing the paradigms of legality and legitimacy of private rulemaking under EU law*, in *CMLR*, n. 4, 2018, p. 1190 ss.

[33] *Global Garden*, sopra citata; Corte giust. 14 dicembre 2017, C-630/16, *Anstar*; 22 febbraio 2018, C-185/17, *SAKSA*; Tribunale 9 luglio 2019, T-53/18, *Germania/Commissione*; Corte giust. 17 dicembre 2020, C-475/19 P e C-688/19 P, *Germania/Commissione*.

[34] Nonostante le norme tecniche siano generalmente coperte da copyright. V. Corte giust. 5 marzo 2024, C-588/21 P, *Public.Resource.Org*, punti 81-87.

[35] M. Eliantonio, *Judicial Control of the EU Harmonized Standards: Entering a Black Hole?*, in *Legal Issues of Economic Integration*, n. 4, 2017, p. 399 ss.; C. Tovo, *op. cit.*, p. 1187

norme armonizzate, per quanto incerto nei suoi contorni, è oggi indiscutibilmente riconosciuto sia dalla dottrina sia dalle istituzioni dell'Unione.

3. *Il rinvio alle norme armonizzate nell'art. 40 AIA e la sua attuazione: dalla proposta al testo del regolamento*

In un contesto generale come quello appena ricordato, in cui lo status giuridico delle norme armonizzate in diritto dell'Unione è soggetto a profondi mutamenti ed interpretazioni evolutive, la Commissione europea nella sua proposta di regolamento ("la proposta")[36] aveva compiuto una precisa scelta politica, non priva di implicazioni e rischi da un punto di vista giuridico, nel decidere di regolare i sistemi di IA come *prodotti* e di farlo attraverso la tecnica legislativa del Nuovo Approccio, facendo ricorso proprio alle norme armonizzate[37]. Per i sistemi AI ad alto rischio, in particolare, la proposta prevede una serie di requisiti al Capo 2 del Titolo III – inclusi obblighi in materia di trasparenza, accuratezza, robustezza e cibersicurezza – il cui rispetto è sottoposto a procedure di valutazione e certificazione ai fini della dichiarazione di conformità UE e dell'apposizione della relativa marcatura CE[38]. Applicare le norme armonizzate ai sensi del regolamento 1025/2012 facilita l'ottenimento della certificazione e, dunque, della marcatura CE, che permette l'immissione sul mercato europeo del sistema IA[39]. Ai sensi dell'art. 40 della proposta, infatti, «i sistemi di IA ad alto rischio che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea si presumono conformi ai requisiti essenziali» stabiliti al Capo 2 del Titolo III.

Questa impostazione è rimasta fondamentalmente invariata durante la

ss.; M. Eliantonio, C. Colombo, *Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?*, in *Maastricht Journal of European and Comparative Law*, n. 2, 2017, p. 323 ss.

[36] 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) 206final, 21 aprile 2021.

[37] S. De Vries, O. Kanevskaia, R. De Jager, *Internal Market 3.0: The "Old" New Approach for Harmonising AI Regulation*, in *EP*, n. 2, 2023, p. 583 ss.; M. Almada, N. Petit, *The EU AI act: A medley of product safety and fundamental rights?*, in *EUI RSC Working Paper*, n. 59, 2023, p. 7.

[38] Su questi ultimi aspetti, v. in particolare il Capo 5 del Titolo III AIA.

[39] Art. 43 proposta.

procedura legislativa e, anzi, il meccanismo e la relativa presunzione di conformità sono stati estesi anche alla nuova categoria dei modelli di IA per finalità generali[40]. Tuttavia, su pressione del Parlamento europeo, il ricorso alle norme tecniche è stato circondato da una serie ulteriori precisazioni per garantire la tutela dell'interesse pubblico e dei diritti fondamentali[41]. Innanzitutto, nei considerando del testo definitivo si insiste sulla necessità che le norme armonizzate riflettano lo "stato dell'arte" e che promuovano l'innovazione, la competitività e la crescita del mercato unico[42]. Inoltre, c'è un'attenzione particolare all'inclusività e alla partecipazione nel processo di normazione tecnica: il comma 3 dell'art. 40 stabilisce ora che «i partecipanti al processo di normazione […] rafforzano la governance multipartecipativa garantendo una rappresentanza equilibrata degli interessi e l'effettiva partecipazione di tutti i portatori di interessi pertinenti». Questa categoria include certamente le associazioni rappresentative della società civile e delle PMI finanziate ai sensi del regolamento 1025/2012[43].

In tal modo, si cerca di mitigare le criticità in tema di trasparenza e partecipazione che, abbiamo visto, tradizionalmente caratterizzano il processo di normazione tecnica. Una tale previsione rischia però di rimanere lettera morta: considerate le condizioni del mercato di sistemi IA, nel quale le competenze tecniche sono estremamente concentrate poiché nelle mani di poche persone tendenzialmente alle dipendenze di un ristretto numero di imprese *big tech* le cui risorse finanziarie sono incomparabili a quelle delle associazioni rappresentative della società civile[44], gli ostacoli pratici all'effettiva partecipazione da parte dei portatori d'interesse si annunciano ancor più insormontabili nel processo di normazione relativo all'AIA di quanto non siano già in altri settori. Chiaramente, nella pratica molto dipenderà anche dalla concreta attuazione da parte di CEN e CENELEC, che per il momento appaiono dimostrare un certo grado di collaborazione e apertura nei confronti delle richieste delle istituzioni dell'Unione e della società civile[45].

[40] Art. 40 (1) AIA. V. anche gli ulteriori prodotti inclusi nell'art. 40 (2) AIA.

[41] Emendamenti del Parlamento europeo, approvati il 14 giugno 2023, alla 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.

[42] Considerando n. 121 AIA.

[43] Come si evince dal riferimento agli articoli 5, 6, e 7 del regolamento 1025/2012, cit.

[44] M. Almada, N. Petit, *op. cit.*, p. 22.

[45] V. ad es. CEN-CENELEC Joint Technical Committee (JTC) 21, Task Group (TG) In-

Anche il ruolo di controllo del sistema di *governance* che ruota attorno alla Commissione europea appare rafforzato rispetto alla proposta. Da un lato, il testo finale stabilisce che la richiesta della Commissione alle OEN deve essere preceduta non soltanto dalla procedura di esame nell'ambito del sistema di comitologia, come già previsto dal regolamento 1025/2012, ma anche da una specifica consultazione dei soggetti interessati, incluso il Forum consultivo e il Comitato europeo per l'intelligenza artificiale stabiliti dal regolamento stesso[46]. Dall'altro, viene esplicitato (con maggior chiarezza anche rispetto al regolamento 1025/2012) che la Commissione è tenuta a svolgere una valutazione del contenuto della norma tecnica prima di procedere alla pubblicazione del suo riferimento in Gazzetta ufficiale[47]. Qualora la norma armonizzata non sia completamente conforme alle disposizioni legislative o alla richiesta, la Commissione può decidere di non pubblicare il riferimento in Gazzetta ufficiale, non facendo così sorgere la presunzione di conformità per quella norma[48].

Inoltre, il regolamento contiene un importante (e innovativo) meccanismo per spingere le OEN ad agire in conformità alle indicazioni delle istituzioni: qualora le OEN non abbiano trasmesso la norma tecnica entro la scadenza stabilita, oppure essa non rispetti la richiesta o «non teng[a] sufficientemente conto delle preoccupazioni in materia di diritti fondamentali», la Commissione europea può adottare atti d'esecuzione *ex* art. 291 TFUE che stabiliscano essi stessi quelle «specifiche comuni» necessarie per dare attuazione al Capo 2 del Titolo III al posto delle norme armonizzate[49]. Benché sia dubbio che la Commissione europea abbia effettivamente le capacità tecniche per sostituirsi alle OEN nel redigere atti così complessi nel loro contenuto tecnico, è chiaro che questa possibilità di emanare specifiche comuni introduce un importante deterrente per le OEN, che potrebbero vedersi private del loro ruolo (e dei relativi compensi)[50] qualora il contenuto delle norme armonizzate non sia sviluppato in linea con i requisiti dell'AIA e della Carta dei diritti fondamentali.

clusiveness, *Artificial Intelligence Standardisation Inclusiveness Newsletter*, n. 1, January 2024.

[46] Art. 40 (2) AIA.

[47] Art. 41 (4) AIA.

[48] V. anche art. 11 regolamento 1025/2012.

[49] Art. 41 (1) AIA.

[50] Per l'elaborazione e la revisione delle norme armonizzate, nonché per molte attività ancillari a questa, le OEN sono finanziate dall'UE tramite sovvenzioni per azione o sovvenzioni di funzionamento, v. art. 15 del regolamento 1025/2012.

3.1. *La richiesta di normazione e la questione dei diritti fondamentali*

Ben prima dell'accordo sul testo finale del regolamento da parte di Parlamento e Consiglio, la Commissione europea ha già emanato una decisione di esecuzione contenente la richiesta di sviluppare norme armonizzate a supporto della politica europea in materia di intelligenza artificiale ("la richiesta")[51] nei confronti di CEN e CENELEC, ovvero due delle tre OEN[52]. La Commissione dunque ha scelto di non coinvolgere ETSI, l'organizzazione astrattamente più competente in materia di intelligenza artificiale (poiché specializzata nel campo delle telecomunicazioni), presumibilmente in conseguenza dei conflitti recenti tra ETSI e la Commissione stessa in relazione alla *governance* dell'organizzazione[53]. La decisione, oltre a contenere la lista delle prime dieci norme armonizzate da sviluppare ai fini della regolazione dell'intelligenza artificiale in UE[54], dettaglia anche i requisiti che le norme tecniche devono rispettare per ottenere la pubblicazione in Gazzetta ufficiale[55].

Tra questi è di particolare interesse l'obbligo di sviluppare, nel programma di lavoro di CEN e CENELEC, azioni che assicurino che le norme tecniche europee siano in conformità con il diritto dell'Unione in materia di diritti fondamentali e protezione dei dati personali[56]. Su questo CEN e CENELEC hanno un obbligo di rendicontazione, dovendo inviare una relazione sui progressi conseguiti ogni sei mesi[57]. Le norme armonizzate stesse, poi, devono minimizzare i rischi per i diritti fondamentali delle persone[58].

[51] Commission Implementing Decision of 22 of May 2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, C (2023) 3215final.

[52] La base giuridica della richiesta è l'art. 10 del regolamento 1025/2012. Benché sia prassi basare le richieste di normazione direttamente su questa disposizione, il fatto che in questo caso sia stata adottata non per dare attuazione ad un atto legislativo già adottato ma genericamente alla politica UE in materia di intelligenza artificiale è, per quanto giuridicamente valido e giustificato da ragioni di urgenza, per lo meno degno di nota.

[53] In particolare, il sistema di partecipazione e voto di ETSI è ritenuto dalla Commissione europea troppo permeabile ad influenze di attori non europei e poco inclusivo nei confronti della società civile. V. M. Gamito, *The role of ETSI in the EU's regulation and governance of artificial intelligence*, in *Innovation: The European Journal of Social Science Research*, 2024, p. 1 ss.

[54] Allegato 1 della richiesta.

[55] Allegato 2 della richiesta.

[56] Art. 2 (1) (b) della richiesta.

[57] Art. 3 (1) della richiesta.

[58] Allegato 2, punto 1, primo paragrafo, della richiesta.

La richiesta, tuttavia, non specifica quali diritti fondamentali debbano essere presi in considerazione e in che modo debbano essere salvaguardati, limitandosi ad un generico riferimento alla Carta dei diritti fondamentali dell'Unione europea e alla legislazione europea applicabile per la tutela dei diritti fondamentali nell'ambito della progettazione e dello sviluppo di sistemi IA. Lo stesso generico riferimento appare come limite alla possibilità per CEN e CENELEC di tenere conto delle norme tecniche che si stanno sviluppando a livello internazionale (ad esempio da parte di ISO) sugli stessi temi[59]. Poiché in queste organizzazioni private internazionali è forte il rischio di *regulatory capture* e di influenza di aziende para-statali o private aventi sede in ordinamenti giuridici nei quali la tutela dei diritti fondamentali è assente o diversa da quella garantita in UE[60], CEN e CENELEC possono fare rinvio a queste norme tecniche internazionali soltanto se questo non reca pregiudizio alla tutela dei valori dell'Unione e dei diritti fondamentali garantiti dalla Carta e dalla legislazione applicabile per la loro tutela[61].

La concreta definizione degli strumenti rilevanti per la protezione dei diritti fondamentali, di quali diritti siano da considerare e come questi vadano bilanciati tra loro non è oggetto di attenzione nella richiesta, così che tali delicatissimi profili sono in buona sostanza rimessi alla valutazione di CEN e CENELEC, senza che criteri oggettivi e condizioni definite *ex ante* ne delimitino la discrezionalità. Nonostante l'effettiva considerazione dei profili di tutela dei diritti fondamentali possa essere successivamente controllata dalla Commissione europea in sede di pubblicazione del riferimento in Gazzetta ufficiale, questa scelta solleva una serie di dubbi di ordine sia pratico sia giuridico. Da un punto di vista pratico, non è affatto chiaro se le OEN abbiano le competenze necessarie per procedere a queste valutazioni. La *ratio* per il coinvolgimento delle OEN nella regolazione dell'Unione tradizionalmente è basata sulle competenze tecniche, scientifiche e informatiche che i loro componenti, a differenza dei funzionari delle istituzioni dell'Unione, possono offrire. La conoscenza del contenuto e del corretto bilanciamento di diritti fondamentali stabiliti dal diritto dell'Unione tendenzialmente esula dalle competenze – e prima ancora, dalla *forma mentis* – di soggetti la cui *expertise* è lontana dalla scienza giuridica. Questa consapevolezza emerge

[59] V. ad es. ISO/IEC 23053:2022 (Framework for Artificial Intelligence Systems Using Machine Learning); IEEE 3129-2023 (IEEE Standard for Robustness Testing and Evaluation of Artificial Intelligence-based Image Recognition Service).

[60] M. Cantero Gamito, *The influence of China in AI governance through standardisation*, in *Telecommunications Policy*, n. 10, 2023.

[61] Allegato 2, punto 1, secondo paragrafo.

dalla richiesta stessa nella quale si prevede che, non avendone già, «CEN and CENELEC shall gather relevant expertise in those areas»[62]. La scelta della Commissione europea dunque appare quella di esternalizzare "alla cieca" un compito di estrema delicatezza, rimettendo alle scelte organizzative delle OEN la definizione di chi, e come, dovrebbe effettuare quelle valutazioni giuridiche.

Giuridicamente, il conferimento del potere di attuare queste valutazioni, il cui impatto sociale, valoriale ed etico oltre che giuridico è evidente, può essere letto come una forma di delega di poteri da parte delle autorità pubbliche ad un ente privato. Pur essendo ammesso dal diritto dell'Unione, un tale potere di delega è sottoposto ai limiti elaborati dalla Corte di giustizia nella sentenza *Meroni*, nella quale si distingue tra la delega di poteri puramente esecutivi «nettamente circoscritti ed il cui esercizio può per ciò stesso venir rigorosamente controllato in base a criteri obbiettivi stabiliti dall'autorità delegante» e «un potere discrezionale che comporti una ampia libertà di valutazione»[63]. Nel secondo caso, una delega di poteri è preclusa poiché potrebbe determinare uno spostamento di responsabilità e minare l'equilibro istituzionale. L'assenza di chiari criteri nell'AIA e nella richiesta, l'ampiezza delle valutazioni rimesse alle OEN nell'elaborazione di norme armonizzate che rispettino i diritti fondamentali della Carta e l'incertezza circa le competenze necessarie all'esercizio di una valutazione giuridicamente complessa ed altamente discrezionale, senza alcuna procedimentalizzazione che garantisca un efficace coinvolgimento di portatori di interessi contrapposti a quelli dell'industria in quei processi di valutazione e bilanciamento *ex ante*, suggeriscono che, nonostante la tecnicità del contenuto delle norme, ancor più che negli altri casi di uso delle norme tecniche a fini regolatori, l'art. 40 AIA deleghi un ampio margine di discrezionalità a questi organismi privati. Ciò rende inoltre il controllo *ex post* della Commissione particolarmente difficile, anche tenuto conto del contenuto tecnicamente complesso delle norme armonizzate per la cui valutazione sostanziale la Commissione, priva delle competenze necessarie al suo interno e del supporto degli esperti nazionali nelle procedure di comitato, dovrà affidarsi (come avviene sistematicamente dal 2018) a soggetti esterni, anch'essi privati[64]. Questo, unito alle difficoltà permanenti in relazione alla possibilità di ricorso diretto nei con-

[62] Allegato 2, punto 1.

[63] Corte giust. 13 giugno 1958, 9/56 e 10/56, *Meroni*, punto 152. V. anche Corte giust. 22 gennaio 2014, C-270/12, *Regno Unito/Parlamento e Consiglio*, punto 75, che tuttavia riguarda la delega ad agenzie dell'Unione e non è dunque applicabile alle OEN.

[64] Gli *HAS consultants*, v. supra nota 16.

fronti delle norme armonizzate, porta a dubitare non solo dell'opportunità di questa scelta legislativa, ma presumibilmente anche della piena compatibilità di questa disposizione con la giurisprudenza della Corte a tutela dei principi generali del diritto dell'Unione europea.

4. *Considerazioni conclusive*

Alla luce di queste riflessioni, appare evidente che il ruolo delle norme tecniche nell'attuazione dell'AIA richiederà una particolare attenzione da parte dei commentatori, per le importanti questioni pratiche e giuridiche che solleva. La scelta di delegare ad organizzazioni private, seppur controllate *ex post* dalle istituzioni dell'Unione, la definizione di norme di dettaglio per l'attuazione del Titolo III, infatti, riguarda una parte significativa dei sistemi IA, ovvero i sistemi ad alto rischio che, per definizione, presentano un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche[65]. È quindi particolarmente importante che le questioni legate alla legittimità delle norme armonizzate – che dipendono non soltanto dall'inclusività e rappresentatività degli attori coinvolti nel processo, ma anche dall'adeguatezza del fondamento giuridico di questa delega sulla base della giurisprudenza della Corte – vengano analizzate criticamente.

Al contempo, la decisione di affidarsi in maniera così significativa alle OEN per la regolazione dei sistemi IA ad alto rischio rappresenta una svolta fondamentale per il ruolo delle norme tecniche armonizzate in diritto dell'Unione, come è stato riconosciuto dalle istituzioni UE[66] e dalla stessa comunità di normazione[67]. Per la prima volta, le norme tecniche verranno utilizzate al di là dello specifico (e relativamente pacifico) ambito della regolazione dei prodotti industriali e dei servizi nel mercato interno, per regolare un vasto ambito tecnicamente ed eticamente complesso quale è quello delle tecnologie digitali più innovative. Il contenuto della normazione tecnica sarà inevitabilmente intriso di valutazioni delicate su valori e diritti fondamentali dell'Unione, con importanti ripercussioni sulla vita degli individui. Inoltre,

[65] V. art. 6 e Allegato III AIA.

[66] Comunicazione della Commissione europea, del 2 febbraio 2022, Una strategia dell'UE in materia di normazione. Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale, COM (2022) 31final.

[67] V. D. Jewell, *Discorso tenuto nel primo incontro dello High-Level Forum on European standardization*, 20 January 2023.

come sottolineato nella recente *Strategia dell'UE in materia di normazione*[68], la normazione tecnica in materia di tecnologie digitali (e di IA in particolare) è attualmente attraversata da intricate tensioni geopolitiche, con "imperi digitali" e organizzazioni private in competizione tra loro per la regolazione di questa nuova frontiera[69]. Anche queste tensioni influenzeranno l'attuazione dell'art. 40 AIA. In questo contesto, il ruolo della normazione tecnica nell'AIA indubbiamente va ben al di là di una mera riproposizione in ambito *tech* della tradizionale tecnica legislativa del Nuovo Approccio[70] e acquisisce nuove dimensioni date dalla complessità tecnica e dall'impatto politico, economico e geo-politico – ma prima ancora giuridico ed etico – come mai la normazione armonizzata ha avuto nel diritto dell'Unione.

[68] COM (2022) 31final, cit.

[69] V. A. Bradford, *Digital Empires*, Oxford University Press, 2023.

[70] V. S. De Vries, O. Kanevskaia, R. De Jager, *op. cit.*, p. 583 ss.

Abstract (ita)

Il presente contributo analizza il ruolo della normazione armonizzata nel quadro del regolamento sull'intelligenza artificiale (AIA). A questo fine ricostruisce brevemente l'evoluzione della tecnica legislativa di rinvio a norme tecniche emanate da organizzazioni private di normazione in diritto dell'Unione, dando conto dei recenti sviluppi giurisprudenziali e dei profili problematici che sono emersi in quest'ambito. L'analisi si concentra poi in dettaglio sul rinvio alle norme armonizzate compiuto in particolare dall'art. 40 AIA per l'attuazione della disciplina relativa ai sistemi IA ad alto rischio ed offre alcune riflessioni sulle implicazioni pratiche e giuridiche del loro uso nell'ambito della tutela dei diritti fondamentali, sollevando rilievi critici sulla compatibilità con la giurisprudenza in materia di delega di poteri e sulle inedite dimensioni etiche, giuridiche e (geo-)politiche che la normazione armonizzata viene così ad assumere nella regolazione delle tecnologie digitali.

Abstract (eng)

This contribution analyses the role of harmonized standardization in the framework of the Artificial Intelligence Act (AIA). It shortly traces the evolution of the legislative technique of referring to technical standards issued by private standardization organizations in EU law, giving account of recent developments in the case law and of the legal issues that have emerged in the field before examining in detail the reference to harmonized standards enshrined in particular in Art. 40 AIA for the implementation of the obligations concerning high-risk AI systems. The analysis offers some reflections on the practical and legal implications of their use in the protection of fundamental rights, questioning its conformity with the case law on the delegation of powers and the unprecedented ethical, legal and (geo-)political dimensions that harmonized standardization thus acquires in the regulation of digital technologies.

IL GIORNO DOPO LA RIVOLUZIONE: PROSPETTIVE DI ATTUAZIONE DEL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE E POTERI DELLA COMMISSIONE EUROPEA

Federico Ferri*

SOMMARIO: 1. Introduzione. – 2. Poteri normativi in un'ottica di contrasto dei rischi alti o sistemici. – 3. Effettività del sistema e potere di infliggere sanzioni. – 4. Cenni alla ramificazione della *governance* sovranazionale in materia di IA. – 5. Rilievi (provvisoriamente) conclusivi.

1. *Introduzione*

Se l'idea di regolamentare l'intelligenza artificiale ("IA") nell'Unione europea rappresenta l'anticamera di una vera e propria "rivoluzione copernicana", l'adozione del regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale[1] (*Artificial Intelligence Act* – "AIA"), dà corpo alla rivoluzione, o quantomeno al suo primo stadio.

La transizione digitale è da anni una priorità indiscussa dell'Unione[2], ma ultimamente sembra essere stata accentuata tanto nella narrativa delle istituzioni UE quanto nella produzione normativa a livello sovranazionale. È comunque evidente che questa accelerazione coincide per larghi tratti con l'impulso che in ambito europeo è stato dato allo sviluppo dell'IA e al dibattito su una eventuale disciplina in materia.

Dal punto di vista istituzionale, la regolamentazione dell'IA è stata invocata a più riprese dalle varie anime rappresentate nell'ordinamento giuridico

* Ricercatore in Diritto dell'Unione europea, *Alma Mater Studiorum* – Università di Bologna.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[2] Per un'analisi giuridica in proposito, si veda C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, pp. 1-34.

dell'Unione[3]. È stato giustamente rimarcato il ruolo propulsivo del Parlamento europeo[4], è nota la spinta offerta dalla Commissione europea[5] e non sono mancate prese di posizione concrete da parte di Consiglio europeo[6] e Consiglio[7]. Tuttavia, questa iniziale comunione di intenti ha via via lasciato spazio a prevedibili divergenze tra istituzioni, affiorate nitidamente durante il faticoso percorso che ha condotto all'adozione del regolamento.

Si ritiene allora d'interesse ragionare su taluni profili istituzionali per immaginare…il giorno dopo la rivoluzione. L'obiettivo di questo lavoro è riflettere su dinamiche suscettibili di prodursi in conseguenza dell'esercizio di *core powers* rivolti a quella complessa «dimensione europea» della regolazione dell'IA, sempre in bilico tra esigenze di non frammentazione del mercato interno e delicati equilibri di tutela dei diritti fondamentali[8]. Nello specifico, ci si propone di ricostruire i capisaldi del ruolo della Commissione europea ai fini dell'attuazione dell'AIA, per fissare alcune coordinate iniziali – ma sufficientemente stabili – in merito al posizionamento del baricentro degli equilibri di potere tra istituzioni e tra livelli.

Allo scopo, tre saranno gli ambiti di indagine da coprire in sequenza: estensione e profondità dei poteri normativi della Commissione (par. 2), portata dei meccanismi sanzionatori (par. 3), peculiarità del livello UE di *governance* (par. 4). Saranno quindi presentate alcune conclusioni (par. 5), in attesa di elementi di prassi negli anni a venire.

Si anticipa che l'analisi sarà realizzata anche tenendo conto degli snodi principali della procedura legislativa e di alcune specificità di regolamenti

[3] Tra l'altro, tra gli obiettivi digitali che il Parlamento europeo, il Consiglio, la Commissione e gli Stati membri devono raggiungere in cooperazione reciproca vi è la trasformazione digitale delle imprese anche in funzione della diffusione dell'IA: decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030.

[4] Si rinvia a G. Di Federico, *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. Di Federico (a cura di), *Alla (ri)scoperta del Parlamento europeo: 1979-2019*, Torino, 2021, pp. 71-88.

[5] Ad esempio, Commissione europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM (2020) 65final, 19 febbraio 2020.

[6] Ad esempio, conclusioni del Consiglio europeo, del 2 ottobre 2020 (riunione straordinaria), EUCO 13/20, punto 13.

[7] Ad esempio, conclusioni della Presidenza del Consiglio, The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, 11481/20, 21 ottobre 2020.

[8] Per considerazioni diffuse sulla questione, si veda C. Schepisi, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, pp. 53-75.

al servizio della transizione digitale UE che con l'AIA condividono obiettivi di fondo e carica innovativa[9]. Ecco che allora talvolta sarà dato risalto anche alla proposta della Commissione europea del 2021[10], all'orientamento generale del Consiglio del 2022[11] e al compromesso raggiunto in seno al Parlamento europeo nel 2023[12]; nello stesso modo, alcuni passaggi saranno sviluppati mettendo a confronto, all'occorrenza, AIA e atti quali la legge sui servizi digitali ("DSA")[13], la legge sui mercati digitali ("DMA")[14] e il regolamento generale sulla protezione dei dati ("GDPR")[15].

2. *Poteri normativi in un'ottica di contrasto dei rischi alti o sistemici*

Il punto di attenzione iniziale è rappresentato dai poteri normativi di cui dispone la Commissione nell'impianto complessivo dell'AIA. Si tratta di attribuzioni certamente rilevanti e che vanno ben oltre la capillarità degli orientamenti attuativi che la Commissione può produrre[16]. Effettivamente,

[9] Circa quest'ultimo aspetto, si ricorda che tali atti fanno parte di quello che in dottrina è stato opportunamente qualificato come un «disegno strategico» di sviluppo del mercato unico digitale e *leadership* normativa dell'Unione su scala mondiale: v. G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, 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*, Milano, 2022, pp. 222-223. Si veda, inoltre, G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021 (*passim*).

[10] Commissione europea, 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) 206final, 21 aprile 2021.

[11] Doc. 14954/22, del 25 novembre 2022. Il testo è consultabile al seguente link: www.data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf.

[12] DRAFT Compromise Amendments, version 1.1, 16 May 2023. Il testo è consultabile al seguente link: www.europarl.europa.eu/resources/library/media/20230516RES90302/20230516RES90302.pdf.

[13] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

[14] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828.

[15] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[16] La Commissione elabora infatti orientamenti diffusi sull'attuazione del regolamento,

la Commissione è nelle condizioni di incidere profondamente sull'operatività dell'AIA, che in assenza di queste misure rischierebbe di risultare inefficace. Il riferimento va dunque in misura principale, sebbene non esaustiva, agli atti delegati e di esecuzione che il TFUE tratta agli artt. 290 e 291 e sui quali il legislatore dell'Unione evidentemente fa leva per favorire il compimento degli obiettivi dell'AIA[17].

Il potere di adottare atti delegati, in concreto, è disciplinato dall'art. 97 AIA, che stabilisce limiti materiali e procedurali. Naturalmente, le prerogative stabilite da questa norma non possono essere espressione di una discrezionalità assoluta della Commissione, visto che gli atti delegati possono essere adottati entro 5 anni dall'entrata in vigore del regolamento e che la delega di potere resta revocabile in qualsiasi momento dal Parlamento europeo o dal Consiglio[18]. Preme comunque ricordare sin da ora che, malgrado la riforma operata con l'art. 290 TFUE abbia teoricamente introdotto una struttura costituzionale più democratica per l'adozione degli atti delegati[19], il sistema della delega di potere non è privo di zone d'ombra[20] e, sul piano operativo, la revoca operata dal delegante è un evento praticamente sconosciuto alla prassi[21].

È allora interessante notare come la Commissione possa adottare atti delegati in numerose situazioni disciplinate dall'AIA[22], specie se si assumono come modelli il GDPR[23] e il DMA[24]; solo il DSA, semmai, può dirsi parago-

come previsto dall'art. 96 AIA.

[17] Solo alla Commissione sono attribuiti tali poteri nell'AIA, nonostante sia ormai pacifico che gli atti *ex* artt. 290 e 291 TFUE possano essere adottati anche da altri soggetti, come le agenzie: cfr. C. Tovo, *Le agenzie decentrate dell'Unione europea*, Napoli, 2016, pp. 69-86, e J. Alberti, *Le agenzie dell'Unione europea*, Milano, 2018, pp. 343-364.

[18] Va precisato che, secondo l'art. 97, par. 2, AIA, la delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

[19] R. Schütze, *'Delegated' Legislation in the (new) European Union: A Constitutional Analysis*, in *The Modern Law Review*, n. 5, 2011, pp. 661-693.

[20] Sul punto, ci si riporta in particolare ai recenti spunti offerti da A. Volpato, *Delegation of Powers in the EU Legal System*, London, 2022.

[21] La tendenza, casomai, è di ricorrere a obiezioni agli atti delegati: v., ad esempio, M. Chamon, *The Legal Framework for Delegated and Implementing Powers Ten Years after the Entry Into Force of the Lisbon Treaty*, in *ERA Forum*, n. 1, 2021, p. 30.

[22] Rispetto alla proposta di regolamento (in particolare, l'art. 73), sono aumentate le ipotesi nelle quali la Commissione può adottare atti delegati, ma l'istituzione non può più esercitare tale potere per un periodo di tempo indeterminato.

[23] Art. 92 GDPR.

[24] Art. 49 DMA.

nabile all'AIA dal punto di vista dell'estensione delle casistiche nelle quali è possibile ricorrere all'esercizio della delega[25]. Non solo. Le fattispecie che possono essere regolate attraverso atti delegati sono decisamente importanti nell'economia dell'AIA, al punto che viene da chiedersi se la Commissione, a dispetto di quanto previsto dall'art. 290 TFUE, abbia modo di integrare o modificare elementi essenziali dell'atto legislativo. Il dubbio, per lo meno, pare lecito sulla scorta di una giurisprudenza abbastanza chiara sugli elementi da appurare in astratto, ma che in ultima analisi tende a subordinare l'apprezzamento finale dell'essenzialità alle specificità del caso concreto[26].

Il nucleo della delega di potere risiede nella gestione del rischio di tipo «alto»[27] oppure «sistemico»[28]. È con atto delegato che la Commissione può modificare l'Allegato III del regolamento, che elenca sistemi ad alto rischio; e la modifica può investire le ipotesi previste o i relativi casi d'uso, come disposto dagli artt. 6, par. 6, e 7, par 1 e par. 3, AIA, soprattutto in funzione del grado di rischio di danno per la salute e la sicurezza, o di impatto sui diritti fondamentali. Sempre a mezzo di atti delegati, la Commissione avrà

[25] Art. 87 DSA.

[26] V., *ex multis*: Corte giust. 5 settembre 2012, C-355/10, *Parlamento/Consiglio*, punti 63-85; 17 marzo 2016, C-286/14, *Parlamento/Commissione*, punti 42-50; 11 maggio 2017, C-44/16, *Dyson/Commissione*, punti 61-62; 26 luglio 2017, C-696/15 P, *Repubblica/Commissione*, punti 71-89.

[27] Le regole di classificazione dei sistemi di IA ad alto rischio sono fissate all'art. 6, par. 1, e all'Allegato III AIA. Tuttavia, tali disposizioni non forniscono dettagli indicativi ai fini della qualificazione del concetto in esame. Si rinvia allora al considerando 46 del regolamento, dal quale emerge che devono essere limitati alla tipologia di alto rischio i sistemi di IA alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, sulla sicurezza e sui diritti fondamentali delle persone nell'UE. Da notare che il considerando n. 48 menziona un insieme decisamente ampio di diritti fondamentali da utilizzare come parametro, includendo anche fattispecie che, ai sensi dell'art. 52, par. 5, della Carta, rilevano come "principi". Inoltre, il considerando 61 crea un canale diretto tra alto rischio e base assiologica dell'Unione, riferendosi a valori fondanti (segnatamente, democrazia e stato di diritto).

[28] L'art. 3, punto 65, AIA definisce il rischio sistemico come un «rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore». Il considerando n. 110 del regolamento avanza alcuni esempi, tra cui i rischi che includono: «qualsiasi effetto negativo effettivo o ragionevolmente prevedibile in relazione a incidenti gravi, perturbazioni di settori critici e serie conseguenze per la salute e la sicurezza pubbliche; eventuali effetti negativi, effettivi o ragionevolmente prevedibili, sui processi democratici e sulla sicurezza pubblica ed economica; la diffusione di contenuti illegali, mendaci o discriminatori».

modo di rivedere la valutazione di conformità dei sistemi di IA ad alto rischio, aggiornando condizioni e procedure[29]. In aggiunta, il ricorso ad atti delegati è previsto per raffinare le regole applicabili ai modelli di IA per finalità generali ("GPAI")[30] con rischio sistemico di cui all'art. 51 AIA: la Commissione ha dunque titolo per modificare criteri ed indicatori sostanziali per la designazione di questi modelli, nonché gli oneri che i rispettivi fornitori devono soddisfare con riguardo alla documentazione tecnica e alle informazioni da fornire[31].

Benché gli interventi passati in rassegna rimangano in parte subordinati alla valutazione di molteplici condizioni, assistite da criteri predefiniti[32] (o, se del caso, alla sussistenza di prove concrete e affidabili[33]), è evidente che la Commissione si trova nella posizione ottimale per rimodulare i cardini del sistema di tutela approntato dal regolamento.

L'approccio appena ricostruito è per larghi tratti rafforzato dalle disposizioni del regolamento che consentono alla Commissione di adottare atti di esecuzione *ex* art. 291 TFUE[34].

Un esempio pertinente è l'art. 41, par. 1, AIA, grazie al quale la Commissione può stabilire, in determinate circostanze, specifiche comuni per i requisiti applicabili ai sistemi di IA ad alto rischio (artt. 8-15). Similmente, qualora non siano stati resi disponibili codici di buone pratiche in tempo utile, l'art. 56, par. 9, autorizza la Commissione ad adottare atti di esecuzione per introdurre norme comuni per l'attuazione degli obblighi che ricadono, in virtù degli artt. 53 e 55, sui fornitori di modelli GPAI, inclusi quelli ad

[29] Art. 45, par. 5 e par. 6, AIA. Il potere di delega può quindi essere esercitato anche sull'Allegato VI (relativo al controllo interno) e sull'Allegato VII (inerente alla valutazione del sistema di gestione della qualità e la valutazione della documentazione tecnica, con il coinvolgimento di un organismo notificato).

[30] L'art. 3, punto 63), AIA li definisce come modelli di IA caratterizzati da «una generalità significativa», che siano in grado di «svolgere con competenza un'ampia gamma di compiti distinti» e che possano essere integrati «in una varietà di sistemi o applicazioni a valle». La disciplina di questi modelli segna uno scarto parziale tra regolamento e proposta.

[31] Artt. 51, par. 3, 52, par. 4, 53, par. 5 e par. 6, oltre agli Allegati XI, XII e XIII AIA.

[32] Si vedano, a titolo di esempio, gli artt. 6, par. 3, e 7, par. 2, AIA.

[33] V., in specie, l'art. 6, par. 6, AIA.

[34] Gli atti di esecuzione cui ci si riferisce nel prosieguo dovranno essere adottati con procedura di comitato e in ossequio all'art. 5 del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (si veda l'art. 98, par. 2, AIA).

alto rischio[35]. Senza dimenticare che un codice di buone pratiche può essere approvato proprio dalla Commissione con atto di esecuzione, anche allo scopo di conferirvi una validità generale all'interno dell'Unione[36]. In più, dai contenuti di apposito atto di esecuzione dipenderà la fisionomia del piano di monitoraggio successivo all'immissione sul mercato dei sistemi di IA ad alto rischio (art. 72, par. 3).

Accanto ai suddetti poteri normativi, vi sono altre prerogative salienti che la Commissione può esercitare nel quadro di attuazione dell'AIA, con precipuo riferimento alle categorie di sistemi di IA ritenute maggiormente pericolose.

Riallacciandosi alle considerazioni sviluppate poco sopra sui modelli GPAI, merita di essere enfatizzato il disposto dell'art. 51, par. 1, lett. b)[37], che permette alla Commissione di decidere, anche *ex officio*, che uno di questi peculiari modelli debba essere classificato con associazione a rischio sistemico; e ancorché siffatto potere sia condizionato al rispetto dell'Allegato XIII, si è visto che la Commissione può certamente arrivare a ridefinire i criteri in esso elencati.

Tutt'altro che marginale è il potere della Commissione di decidere che l'autorità di vigilanza del mercato di uno Stato membro ritiri l'autorizzazione eventualmente rilasciata per consentire, a livello nazionale e in via di deroga, l'immissione sul mercato o la messa in servizio di specifici sistemi di IA ad alto rischio per motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente o dei principali beni industriali e infrastrutturali[38]. Secondo questa logica, la Commissione detiene altresì poteri in relazione all'autorizzazione un organismo di valutazione della conformità notificato dall'autorità interna[39].

Infine, molto incisiva pare essere la clausola di salvaguardia «dell'Unione» elaborata nell'AIA all'art. 81 per innalzare il livello di tutela contro i rischi presentati da sistemi di IA non conformi (ulteriormente sviluppata dall'art. 82 per i sistemi di IA conformi). In situazioni transfrontaliere che sollevano contrasti tra più autorità di vigilanza del mercato, la Commissione può agire persino in prima persona per decidere se sia o meno giustificata una misura interna che abbia conseguenze provvisorie o definitive per il fornitore considerato[40].

[35] Sono questi i contenuti più rilevanti dei codici di buone pratiche, in base a quanto si ricava dall'art. 56, par. 2, AIA.

[36] Art. 56, par. 6, AIA.

[37] Si veda anche l'art. 52, par. 4, AIA.

[38] Si veda l'art. 46 AIA, con enfasi sui rispettivi par. 5 e par. 6.

[39] Si rinvia in particolare agli artt. 30, 36 e 37 AIA.

[40] Ad esempio, l'art. 79, par. 5, AIA sancisce che, stanti varie condizioni di carattere so-

3. *Effettività del sistema e potere di infliggere sanzioni*

Tra le manifestazioni dei poteri con i quali la Commissione ha modo di innalzare il grado di effettività delle tutele stabilite dall'AIA vi sono le sanzioni per i fornitori di modelli GPAI. Rileva dunque l'art. 101 del regolamento, che completa le disposizioni che disciplinano forme e limiti del controllo nei confronti di questa particolare tipologia di operatori. Detto articolo costituisce una novità delle fasi conclusive della procedura legislativa e si aggiunge alle disposizioni del Capo XII, concernenti le sanzioni che possono essere inflitte dagli Stati membri contro «operatori» in generale (art. 99)[41] e del Garante europeo per la protezione dei dati contro istituzioni, organi e organismi dell'Unione (art. 100).

L'art. 101 AIA (a differenza dell'art. 99) menziona unicamente sanzioni pecuniarie, le quali costituiscono titolo esecutivo a tenore dell'art. 299 TFUE[42]. Al netto del rispetto dei principi di proporzionalità e adeguatezza, della presenza di indicatori che la Commissione deve seguire per stabilire l'importo della sanzione e di accorgimenti procedurali che concretizzano i diritti dell'interessato, il par. 1 dell'art. 101 dispone che le sanzioni possono essere irrogate solo se la violazione sia stata intenzionale o sia occorsa per negligenza. Sono anche stabilite soglie massime di importi: non è consentito oltrepassare il 3% del fatturato mondiale totale dell'esercizio precedente del fornitore o i 15 milioni di euro (se superiore).

Le sanzioni pecuniarie di cui trattasi possono essere adottate con decisione, secondo modalità procedurali che la Commissione dovrà circostanziare con un atto di esecuzione. Si precisa poi che le decisioni che fissano tali sanzioni pecuniarie potranno essere sottoposte al sindacato della Corte di giustizia, che avrà facoltà di intervenire nel merito ed estinguere o modificare l'importo individuato in precedenza dalla Commissione. Molto più blando sembra invece il ruolo di altri organi a questo proposito: ad esempio, l'art. 101 richiama il Comitato europeo per l'intelligenza artificiale (su cui si ritornerà a breve), ma solo per consentirgli di ricevere, «se del caso», infor-

stanziale e procedurale, l'autorità di vigilanza del mercato «adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato nazionale, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo».

[41] Si precisa che le sanzioni *ex* art. 99 AIA devono essere predisposte tenendo in conto appositi orientamenti che la Commissione adotta in ossequio all'art. 96.

[42] Lo stesso art. 299 TFUE, al secondo paragrafo, aggiunge che l'esecuzione forzata è regolata dalle norme di procedura civile vigenti nello Stato sul cui territorio essa viene effettuata.

mazioni in merito alle sanzioni pecuniarie inflitte dalla Commissione.

Nel quadro dell'art. 101 la Commissione ha il potere comminare sanzioni pecuniarie a fornitori di modelli GPAI per violazioni «delle pertinenti disposizioni» del regolamento. Ci sono poi ipotesi specifiche di violazioni che possono culminare con l'imposizione di sanzioni riconducibili all'art. 101. Rientra in questa casistica l'inerzia del fornitore di fronte alla richiesta di porre in atto le misure elencate all'art. 93, l'omessa trasmissione alla Commissione di documenti o informazioni (art. 91, par. 4), la mancata fornitura dell'accesso al modello in questione allo scopo di effettuare una valutazione di conformità al regolamento (art. 92, par. 4).

Di conseguenza, nell'impostazione dell'art. 101 AIA diviene evidente la prosecuzione di un approccio messo in atto in epoca *post*-GDPR[43], e che propone una collocazione sempre più salda della Commissione europea al centro dei meccanismi di controllo di alcuni tra i principali strumenti della normativa UE sul digitale. In proposito, rileva il parallelismo tra poteri sanzionatori della Commissione nei regolamenti su intelligenza artificiale, da un lato, e servizi e mercati digitali, dall'altro.

Le similitudini si colgono soprattutto con il DSA. Prendendo in esame l'art. 74 di questo regolamento, si rinvengono prerogative analoghe che la Commissione può esercitare contro i fornitori di piattaforme *online* e di motori di ricerca *online* di dimensioni molto grandi[44]. Anche in questo caso, la Commissione può intervenire per assicurare l'effettività delle proprie decisioni di non conformità (a norma dell'art. 73) per qualsiasi violazione intenzionale o negligente degli obblighi imposti dall'atto legislativo. E malgrado nel DSA i massimali delle sanzioni siano tendenzialmente più alti rispetto a quelli specificati dall'art. 101 AIA, le differenze sostanziali e procedurali tra i due sistemi sono lievi. Qualche variazione in più si rinviene, invece, mettendo a confronto AIA e DMA, se non altro perché l'art. 30 del secondo

[43] Circa il tema delle sanzioni nel quadro del GDPR si rinvia a P. De Hert, *EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism*, in S. Montaldo, F. Costamagna, A. Miglio (eds.), *EU Law Enforcement: the Evolution of EU Sanctioning Powers*, London – New York – Torino, 2020, pp. 291-324. Si vedano, inoltre, le linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR – Versione 2.1 – adottate il 24 maggio 2023 (www.edpb.europa.eu/system/files/202401/edpb_guidelines_042022_calculationofadministrativefines_it_0.pdf).

[44] Tali concetti sono ricostruibili dal combinato disposto degli artt. 3, lett. i e lett. j, e 33, DSA. È poi la Commissione, in concreto, a designare le piattaforme *online* e i motori di ricerca *online* di dimensioni molto grandi.

si riferisce ad ammende[45] che la Commissione può applicare in ipotesi selezionate e principalmente (ancorché non esclusivamente) contro i cosiddetti *gatekeepers*[46].

In virtù di ciò, l'art. 101 AIA conferma che è in via di sviluppo l'affermazione di una funzione di vigilanza a tratti "rafforzata"[47], che si estende a fattispecie che vanno al di là delle eventualità espressamente previse dai Trattati istitutivi circa le sanzioni derivanti, in via mediata o diretta, dai poteri di controllo della Commissione: ci si riferisce specialmente alle condanne degli Stati membri al pagamento di somme pecuniarie in esito a procedure di infrazione previste dall'art. 260 TFUE[48], o a procedimenti volti alla pronuncia di provvedimenti provvisori secondo l'art. 279 TFUE, nonché alle ammende inflitte a imprese in attuazione della politica UE di concorrenza[49].

La tendenza in atto connota quel processo che in dottrina è stato riassunto come «the creation of a regulatory framework that allows EU authorities to pinpoint and sanction technology companies for a range of con-

[45] L'art. 31, a sua volta, disciplina le penalità di mora.

[46] L'essenza del concetto si rinviene dal combinato disposto degli artt. 2, punto 1), e 3, DMA. Ulteriori specifiche sono contenute al predetto art. 3.

[47] Tra gli esempi recenti di atti legislativi che affidano alla Commissione il potere di infliggere sanzioni a soggetti privati, si segnalano: regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (art. 85); regolamento (UE) 2019/5 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che modifica il regolamento (CE) n. 726/2004 che istituisce procedure comunitarie per l'autorizzazione e la sorveglianza dei medicinali per uso umano e veterinario e che istituisce l'agenzia europea per i medicinali, il regolamento (CE) n. 1901/2006 relativo ai medicinali per uso pediatrico e la direttiva 2001/83/CE recante un codice comunitario relativo ai medicinali per uso umano (art. 84 bis); regolamento (UE) 2022/2560 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alle sovvenzioni estere distorsive del mercato interno (artt. 17 e 26).

[48] Si veda anche comunicazione della Commissione, Sanzioni pecuniarie nei procedimenti d'infrazione (2023/C 2/01). Per approfondimenti, sul tema si rinvia a M. Condinanzi, C. Amalfitano, *La procedura di infrazione dieci anni dopo Lisbona*, in *federalismi.it*, n. 19, 2020, pp. 216-300.

[49] Art. 103 TFUE e art. 23 regolamento (CE) n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del trattato, (cf. anche orientamenti per il calcolo delle ammende inflitte in applicazione dell'articolo 23, paragrafo 2, lettera a), del regolamento (CE) n. 1/2003). In argomento, v. P. Manzini, *Le ammende*, in B. Cortese, F. Ferraro, P. Manzini (a cura di), *Il diritto antitrust dell'Unione europea*, Torino, 2014, pp. 259-281.

troversial practices that fly in the face of EU interests»[50]. In particolare, alla radice vi è l'esigenza di tutelare in maniera incisiva l'effettività del diritto UE in situazioni di significativa delicatezza, soprattutto laddove l'evoluzione del progresso tecnologico rischi di entrare in rotta di collisione con i diritti fondamentali riconosciuti e garantiti dalla Carta di Nizza[51] e persino con i valori fondanti enunciati all'art. 2 TUE.

4. *Cenni alla ramificazione della* governance *sovranazionale in materia di IA*

La posizione apicale della Commissione nell'articolato sistema di attuazione dell'AIA si evince anche dalla conformazione del livello UE di *governance*[52], i cui tratti essenziali muovono dall'architettura – relativamente meno sofisticata – del DSA[53]. Il *focus* sulla *governance* è motivato anche dall'attenzione riposta dalla giurisprudenza al tema nella sua più ampia declinazione della transizione digitale europea, come dimostra l'eco della recente sentenza *Meta Platfoms*[54].

Oltre che per il ruolo incisivo che la Commissione può esercitare direttamente, tale sistema si connota anzitutto per la presenza dell'Ufficio per l'intelligenza artificiale (di seguito, "Ufficio"), un organo frutto di una complessa evoluzione dell'*iter* legislativo. In generale, si tratta di una novità di primo piano, in quanto l'Ufficio non era stato contemplato nella proposta della Commissione. Nemmeno il Consiglio, nella posizione espressa a fine 2022, aveva optato per inserire riferimenti in tal senso nel corpo del regolamento da adottare. Diversamente, la scelta di prevedere l'Ufficio si deve per lo più al Parlamento europeo, che auspicava l'aggiunta di un organismo dell'Unione dotato di poteri e funzioni rilevanti[55]. Ebbene, l'emendamento

[50] H. Roberts, J, Cowls, F. Casolari, J. Morley, M. Taddeo, L. Floridi, *Safeguarding European Values with Digital Sovereignty: an Analysis of Statements and Policies*, in *Internet Policy Review*, n. 3, 2021, p. 14.

[51] V. diffusamente C. Grieco, *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023.

[52] Si precisa sin da ora che non è questa la sede per discutere specificità e attori della *governance* nazionale: si rinvia quindi al contributo di S. Villani, in questo *fascicolo speciale*.

[53] Sul punto, sia permesso di rinviare a F. Ferri, *La gouvernance du Digital Services Act et la coopération des autorités*, in *RAE*, n. 3, 2023, spec. pp. 645-648.

[54] Corte giust. 4 luglio 2023, C-252/21, *Meta Platforms e a.* Per approfondimenti sulla pronuncia, cfr. P. Manzini, *Antitrust e privacy: la strana coppia*, in *I Post di AISDUE*, n. 10, 15 settembre 2023, pp. 196-220.

[55] DRAFT Compromise Amendments, cit., art. 56.

può dirsi oggi concretizzato solo in parte, giacché nell'AIA la fisionomia dell'Ufficio è ben diversa dal modello immaginato dal Parlamento europeo. Le ragioni di quanto si sostiene dipendono principalmente dal grado di condizionamento della Commissione rispetto all'organo in commento.

In primo luogo, nel disegno del Parlamento europeo l'Ufficio avrebbe dovuto agire in totale indipendenza e costituire una sorta di compromesso tra istanze diverse. A riprova di ciò, basti pensare che controllo e direzione strategici dell'organo avrebbero dovuto essere affidati agli Stati membri assieme a Commissione, Garante europeo della protezione dei dati, Agenzia europea dei diritti fondamentali e Agenzia dell'Unione europea per la cibersicurezza[56]. In più, si disponeva che l'Ufficio fosse responsabile nei confronti di Parlamento europeo e Consiglio, sì da coinvolgere il più possibile le istituzioni politiche dell'Unione nella *governance* di una IA armonizzata. Al contrario, questa impostazione nell'AIA può dirsi completamente superata. Dal combinato disposto degli artt. 64 e 3, punto 47), del regolamento, si ottiene infatti che l'Ufficio è parte integrante della Commissione: il primo è di fatto una «funzione» attraverso la quale la seconda sviluppa le competenze e le capacità dell'Unione nel settore dell'IA. Vengono meno anche i riferimenti all'*accountability* verso altre istituzioni e, dal canto loro, gli Stati membri possono al massimo «agevolare» i compiti che l'Ufficio è chiamato ad esercitare.

Un ulteriore aspetto che vale la pena evidenziare è la fonte che stabilisce l'Ufficio per l'IA. In effetti, l'AIA si limita a spiegare cos'è l'Ufficio e tutt'al più fissa alcune regole in ordine sparso ogni volta che occorre ricondurre ai compiti dell'organo una determinata tematica oggetto di specifici capi o sezioni del regolamento. L'atto di riferimento, dunque, non è (solamente) l'AIA, ma (principalmente) la decisione istitutiva C/2024/390 della Commissione europea[57].

Da questa decisione, però, emerge già di primo acchito una circostanza piuttosto singolare. Essa si fonda in via generale sul TFUE e nella parte motivazionale fa al massimo qualche timido richiamo ad atti legislativi con cui sono stati introdotti programmi quadro o strategici. L'atto da cui tale decisione dovrebbe trarre la sua ragion d'essere sarebbe, logicamente, l'AIA. Tuttavia, la decisione C/2024/390 è stata adottata nel gennaio del 2024 ed è entrata in vigore un mese dopo; in altre parole, la decisione che istituisce l'Ufficio precede il regolamento sull'IA. Ne consegue, tra l'altro, che la

[56] *Ibidem*, considerando n. 76.

[57] Decisione della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale, C/2024/390, del 14 febbraio 2024.

stessa non può essere intesa né come atto esecutivo né come atto delegato rispetto all'AIA. Ora, benché una simile misura non sia del tutto sconosciuta alla prassi[58], si sostanzia pur sempre in una iniziativa decisamente inconsueta all'interno della categoria – peraltro niente affatto monolitica – delle fonti di diritto derivato dell'Unione.

Ma vi è di più. Preso atto che l'Ufficio per l'IA non è un ufficio europeo ai sensi dell'art. 2, punto 26), del regolamento finanziario[59], il concetto di funzione riportato poc'anzi dovrebbe essere ricondotto, a rigor di logica, ad una manifestazione dell'autonomia istituzionale della Commissione, e quindi al regolamento interno della medesima[60], adottato *ex* art. 249 TFUE. Eppure, anche questo collegamento presta il fianco ad ambiguità, poiché l'art. 22 del regolamento interno, come modificato nel 2010[61], prevede che funzioni e strutture della Commissione possano essere istituite per «esigenze particolari» e sottolinea che tale facoltà è riservata al Presidente dell'istituzione.

Dal momento che la decisione istitutiva dell'Ufficio non proviene dal Presidente della Commissione e non fornisce dettagli su eventuali fondamenti normativi o circostanze idonee a integrare le suddette esigenze particolari, si ritiene che si tratti di un atto in buona parte "a schema libero" e sintomatico del margine di manovra che la Commissione si è riservata nell'attività di supervisione di una materia altamente sensibile.

Ciò trova conferma anche nei contenuti chiave della decisione C/2024/390, cioè le disposizioni che sanciscono i compiti dell'Ufficio per l'IA (segnatamente gli artt. 2 e 3) e che fanno di quest'organo «il centro di competenze in materia di IA in tutta l'UE»[62]. In sintesi, il ruolo dell'Ufficio è senza dubbio strategico, segnatamente per quanto riguarda lo sviluppo di strumenti, metodologie e parametri di riferimento per la valutazione delle capacità dei modelli di IA per finalità generali. Parallelamente, l'Ufficio figura quale struttura incaricata della vigilanza dei progressi compiuti nel campo dei modelli di IA: si occupa del monitoraggio relativo alla comparsa di nuovi rischi e, più in generale, all'applicazione delle norme pertinenti, senza dimenticare che dispone di poteri di indagine su eventuali violazioni.

[58] Si cita, ad esempio, la decisione della Commissione, del 16 settembre 2021, che istituisce l'Autorità per la preparazione e la risposta alle emergenze sanitarie 2021/C 393.

[59] Nota 6 in calce alla decisione C/2024/390, cit.

[60] Regolamento interno della Commissione [C (2000) 3614].

[61] Decisione 2010/138 (UE, Euratom) della Commissione, del 24 febbraio 2010, recante modifica del suo regolamento interno.

[62] www.digital-strategy.ec.europa.eu/it/policies/ai-office.

Tali prerogative sono declinate mediante numerose funzioni di assistenza, sostegno tecnico e coordinamento. Il tutto in un'ottica di cooperazione ad ampio spettro (artt. 4-7 della decisione), in cui l'Ufficio si situa al centro di dinamiche di relazione che spaziano dalla dimensione intersettoriale a quella interistituzionale, per poi estendersi al raccordo con il livello nazionale (inclusi i portatori di interessi) e con Stati terzi e organizzazioni internazionali.

Nell'esecuzione dei propri compiti l'Ufficio è assistito anche da un gruppo di esperti scientifici indipendenti, che arricchisce il sistema di *governance* dell'AIA. Sennonché, questo *pool* di esperti di settore è assoggettato in larga misura ai poteri normativi della Commissione, la quale, in base all'art. 98 AIA, ne seleziona i membri e stabilisce disposizioni organizzative di varia natura.

L'essenza dell'Ufficio differisce da quella del secondo organo che concorre a realizzare la *governance* sovranazionale dell'AIA, ossia il Comitato europeo per l'intelligenza artificiale (di seguito, il "Comitato"). Inserito agli artt. 65 e 66 del regolamento come una specie di "contrappeso" rispetto all'Ufficio[63], il Comitato si compone di un rappresentante per ciascuno Stato membro[64] e la disciplina ad esso applicabile risulta significativamente diversa da quanto prospettato nella proposta della Commissione[65] e nel compromesso raggiunto nel 2023 dal Parlamento europeo[66].

Per un verso, è vero che il Comitato risulta essere maggiormente immune al condizionamento della Commissione. In effetti, non sfugge che nella proposta dell'AIA a quest'ultima venivano (auto)affidate la presidenza del Comitato (che implicava la partecipazione diretta all'approvazione del regolamento interno) e l'autonomia di decisione circa la convocazione delle riunioni e la preparazione dell'ordine del giorno. Ora, invece, la Commissione

[63] Si veda anche www.data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf, p. 7, oltre che l'orientamento generale del Consiglio, del 25 novembre 2022 (doc. 14954/22, cit., spec. p. 8 e considerando n. 76).

[64] L'AIA non dispone, a differenza della proposta, che il Comitato annoveri le autorità nazionali di controllo, ciascuna presente nella persona del rispettivo capo o di un alto funzionario di livello equivalente. Inoltre, ai sensi dell'art. 65 AIA, il Garante europeo della protezione dei dati non è titolare di diritti di voto, ma può al massimo partecipare alle riunioni dell'organo assieme all'Ufficio e, se del caso, di autorità, organismi o esperti nazionali e dell'Unione che abbiano ricevuto un invito *ad hoc*.

[65] DRAFT Compromise Amendments, cit. Ci si riferisce in particolare ai rispettivi artt. 57 e 58.

[66] *Ibidem*. Ci si riferisce in particolare ai rispettivi artt. 57b e 57c, che riproducevano un articolato tentativo di conciliazione tra poteri e funzioni dei diversi poli di rappresentanza presenti nel Comitato.

può partecipare ai lavori del Comitato in maniera essenzialmente indiretta: in parte attraverso l'Ufficio, che provvede al massimo alle funzioni di segretariato, in parte nominando i membri del forum di cui all'art. 67 AIA, che sostiene il Comitato (ma anche la Commissione stessa) fornendo consulenza e competenze tecniche[67].

D'altro canto, però, non vi è dubbio il Comitato sia stato pensato fondamentalmente come un organo di consulenza e supporto[68] di minor peso specifico rispetto all'Ufficio. Questo limite persiste anche se nell'AIA si è avuta una vistosa estensione dei compiti che il Comitato «può» svolgere, fermo restando che l'art. 66 non contiene un elenco chiuso: tra gli esempi più rilevanti in tal senso, si segnalano la possibilità di incidere sull'armonizzazione delle pratiche amministrative a livello nazionale e formulare raccomandazioni e pareri scritti su qualsiasi questione pertinente relativa all'attuazione del regolamento.

5. *Rilievi (provvisoriamente) conclusivi*

Dall'analisi compiuta nei precedenti paragrafi emerge il consolidamento di quel processo di "centralizzazione"[69] che, nel vasto campo del digitale, sta innervando le riforme UE intese a limitare la libertà di azione di attori economici ritenuti capaci di alterare sin dalle fondamenta le basi comuni su cui si innesta il processo di integrazione europea. La "posizione dominante" (sia concessa questa metafora) che la (nuova) Commissione può assumere in sede di attuazione dell'AIA altro non è che la prosecuzione di un approccio in corso di sperimentazione con il DSA e il DMA[70] e che prende le distanze dai meccanismi di *enforcement* a trazione nazionale che contrassegnano il

[67] Il forum consultivo ricomprende rappresentanti di portatori di interessi. Maggiori informazioni al riguardo sono disponibili nel contributo di G. Rugani, in questo *fascicolo speciale*.

[68] Nel testo del regolamento risulta ampliata la gamma dei beneficiari delle funzioni dell'AIA: in base all'art. 66, il Comitato si rivolge non soltanto alla Commissione, ma anche gli Stati membri.

[69] Per conferme in dottrina, v. C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi, A *Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *SSRN*, 5 May 2024 (www.papers.ssrn.com/sol3/papers.cfm?abstract_id=4817755).

[70] Si rinvia alle considerazioni rese in occasione della pubblicazione delle proposte dei regolamenti da M. Eifert, A. Metzger, H. Schweitzer, G. Wagner, *Taming the Giants: the DMA/DSA Package*, in *CMLR*, n. 4, 2021, pp. 987-1028.

GDPR[71]. Stanti grado e ampiezza dei poteri decisionali ad essa attribuiti, nell'arco della trasformazione digitale dell'Unione la Commissione diviene allora più che mai guardiano dei Trattati, oltre che istituzione dotata di poteri a tratti quasi para-legislativi. Questo, almeno, pare essere lo scenario in divenire, sublimato, appunto, dall'adozione dell'AIA.

Un'efficace chiave di lettura per appurare il senso di queste linee evolutive è da rinvenirsi con tutta probabilità nella prima fase del sistema di gestione del rischio, inteso in senso lato. Se l'AIA condivide con i regolamenti appena richiamati – *in primis* con il DSA – l'obiettivo di proteggere la base valoriale dell'Unione[72] e il fatto di essere espressione tangibile del costituzionalismo digitale europeo[73], innova rispetto ad essi anche e soprattutto perché, come argomentato in dottrina, si fonda su un «*top-down risk approach*», evincibile già nella fase di valutazione[74]. A ciò si aggiunge l'evidente complessità dell'oggetto da regolamentare, caratterizzato dall'incessante evoluzione tecnologica e dalle ricadute su rapporti multidirezionali tra soggetti pubblici e privati. Ne deriva che l'Unione, specialmente attraverso la Commissione, si riserva di fissare a monte le regole basilari, di attuarle in un'ottica quanto più unitaria e, se del caso, di rivederle ricorrendo a uno strumentario che offra garanzie di flessibilità operativa.

Tale visione suggerisce che le logiche che permeano l'AIA e che ne informeranno l'attuazione abbiano carattere pseudo-emergenziale. È allora opportuno ricordare che la prassi UE emersa in occasione della gestione di una delle più vistose emergenze degli ultimi decenni, vale a dire la pandemia di COVID-19, lascia intendere che l'affermazione di un contesto emergenziale agevola oltremodo l'insorgere di conseguenze costituzionalmente rilevanti. Su tutte, il ricorso a meccanismi e soluzioni che esprimono una rilettura quantomeno parziale del principio di attribuzione delle competenze[75] e la marginalizza-

[71] Sul punto, si rinvia alle riflessioni di F. Brito Bastos, P. Palka, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, in *ECLR*, n. 3, 2023, pp. 485-517.

[72] Si cita l'opinione di chi sostiene che sin dalla pubblicazione della relativa proposta, il DSA poteva essere visto «a human-rights-infused regulation […] because not only does it explicitly mention the Charter of Fundamental Rights, it also builds in the values of the Charter in the provisions themselves»: P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in T. Flew, F. R. Martin (eds.), *Digital Platform Regulation: Global Perspectives on Internet Governance*, Cham, 2022, p. 76.

[73] G. De Gregorio, O. Pollicino, *The European Constitutional Road to Address Platform Power*, in *verfassungsblog.de*, 31 August 2021.

[74] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, n. 2, 2022, spec. pp. 488-500.

[75] V. *amplius* F. Casolari, *L'Unione europea e la gestione dei disastri: considerazioni di*

zione del Parlamento europeo in luogo di un'accresciuta dimensione della Commissione, riscontrabile tanto nel rapporto tra istituzioni quanto nelle relazioni tra UE e Stati membri[76].

Perciò, con l'avvio definitivo della regolamentazione sovranazionale dell'IA si accentuano ulteriormente le peculiarità della Commissione nel panorama istituzionale e delle organizzazioni internazionali e riecheggiano più che mai le parole di chi presenta questa istituzione come un organo politico che funge da motore del processo di integrazione europea e la cui azione oramai «si atteggia complessivamente come un'azione di governo»[77].

L'auspicio è che, nell'attuazione dell'AIA, tale missione si ispiri a quel principio di «precauzione costituzionale» volto ad evitare il verificarsi di gravi violazioni ai diritti fondamentali[78]. Parimenti, occorre che essa si realizzi il più possibile sotto l'egida di una dimensione democratica effettiva in termini di partecipazione ai processi decisionali e di controllo, in vista di trasformazioni di notevole impatto per i cittadini dell'Unione e, più diffusamente, per gli individui.

natura sistemica a partire dalla reazione sovranazionale alla pandemia di COVID-19, in *CI*, n. 2, 2023, pp. 249-270.

[76] Emblematico è stato il processo di affermazione del piano di ripresa "Next Generation EU". Per considerazioni al riguardo, si vedano: G. Contaldi, *La normativa per l'attuazione del programma Next Generation EU*, in *SIE*, n. 2, 2021, pp. 245-266; F. Costamagna, *Il Next Generation EU e la costruzione di una politica economica europea: quale ruolo per democrazia e solidarietà?*, in *I Post di AISDUE*, n. 3, 15 dicembre 2021, pp. 38-46.

[77] R. Adam, A. Tizzano, *Manuale di diritto dell'Unione europea*, Torino, 2020, p. 101.

[78] Ci si rifà ad A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in A. D'Aloia (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2020, pp. 198-200.

Abstract (ita)

Il presente contributo analizza i profili di maggior rilievo dei poteri che la Commissione europea potrà esercitare nel quadro del regolamento sull'intelligenza artificiale (AIA). L'oggetto dello studio si colloca nel più ampio ambito della *governance* sovranazionale della transizione digitale dell'Unione. Il fine è comprendere se e fino a che punto stia avvenendo un cambio di paradigma a questo proposito, in ragione degli obiettivi da conciliare e dei rischi da contrastare. In particolare, l'analisi si focalizza sui poteri normativi e sanzionatori a disposizione della Commissione, oltre che sugli organi istituiti per favorire il processo di "centralizzazione" dell'attuazione del regolamento.

Abstract (eng)

This contribution analyzes the most important aspects of the powers that the European Commission will be able to exercise within the framework of the Regulation on Artificial Intelligence (AIA). The object of the study falls within the scope of the supranational governance of the digital transition of the Union. The aim is to understand if and to what extent a paradigm shift is taking place in this regard, based on the objectives to be reconciled and the risks to be countered. In particular, the analysis focuses on the regulatory and sanctioning powers of the Commission, as well as on the bodies established to facilitate the process of "centralization" of the implementation of the Regulation.

IL SISTEMA DI VIGILANZA SULL'APPLICAZIONE DELL'*AI ACT*: OGNUN PER SÉ?

Susanna Villani[*]

SOMMARIO: 1. Introduzione. – 2. Il sistema di vigilanza sull'applicazione dell'*AI Act* a livello nazionale. – 3. La vigilanza sull'applicazione dell'*AI Act* da parte dell'Unione: il Garante europeo per la protezione dei dati. – 4. Sistema di vigilanza e strumenti di cooperazione tra autorità. – 4.1. *Segue*: a livello intrastatale. – 4.2. *Segue*: a livello interstatale e sovranazionale. – 5. Riflessioni conclusive.

1. *Introduzione*

Il complessivo sistema di *governance* previsto dal regolamento sull'intelligenza artificiale (di seguito: *AI Act* o regolamento 2024/1689)[1] si articola su un doppio livello: quello sovranazionale e quello nazionale. Il livello sovranazionale comprende quattro nuove strutture (l'Ufficio per l'IA presso la Commissione[2], il Comitato europeo per l'IA composto da rappresentanti degli Stati membri, l'*Advisory Forum* composto dagli *stakeholders* e il Comitato Scientific formato da esperti scientifici scelti dalla Commissione); mentre il livello nazionale si affida ad un'autorità di notifica e ad un'autorità di vigilanza del mercato operante conformemente al reg. (UE) 2019/1020[3].

Il presente contributo si concentrerà specificamente sul sistema di vi-

[*] Ricercatrice in Diritto dell'Unione europea, *Alma Mater Studiorum* Università di Bologna. Ricerca parzialmente finanziata dal programma PNRR – M4C2 – Investimento 1.3, Partenariato Esteso PE00000013 – "FAIR – Future Artificial Intelligence Research" – Spoke 8 "Pervasive AI", finanziato dalla Commissione europea nell'ambito del NextGeneration EU Programme.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[2] L'Ufficio è già stato istituito con decisione C/2024/390 della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale. Per approfondimenti, si rinvia al contributo di F. FERRI, in questo *fascicolo speciale*.

[3] Regolamento (UE) 2019/1020, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011.

gilanza nazionale e sovranazionale e sui compiti attribuiti alle autorità di vigilanza sull'attuazione del regolamento successivamente all'immissione nel mercato dei sistemi di IA e, dunque, finalizzata a completare il meccanismo di controllo e verifica precedente all'utilizzo di detti sistemi; un meccanismo, questo, basato essenzialmente su obblighi a carico degli operatori privati[4]. Infatti, il regolamento prevede che, una volta immessi nel mercato, i sistemi di intelligenza artificiale siano monitorati da una struttura di natura pubblica per garantire l'applicazione corretta ed uniforme della normativa dell'Unione ed, eventualmente, per intervenire rapidamente in caso di rischi imprevisti.

L'obiettivo di tale analisi è duplice: tracciare gli elementi principali di detto sistema di vigilanza e indicare i principali elementi di tensione tra il rispetto dell'autonomia organizzativa degli Stati membri e le esigenze di coerenza sovranazionale nell'attuazione del regolamento da poco adottato. A tal fine, verranno innanzitutto illustrate le funzioni delle autorità di vigilanza da stabilirsi a livello nazionale (par. 2) nonché quelle del Garante europeo per la protezione dei dati quale autorità di vigilanza designata per le istituzioni dell'Unione (par. 3). Delineato il quadro complessivo dell'attività di vigilanza, si passerà ad approfondirne le principali criticità, specialmente rispetto al coordinamento tra le diverse autorità tanto a livello nazionale quanto sovranazionale (par. 4) per poi chiudere con delle riflessioni conclusive (par. 5).

2. *Il sistema di vigilanza sull'applicazione dell'AI Act a livello nazionale*

L'art. 70 del reg. 2024/1689 impone agli Stati membri di designare una o più autorità nazionali competenti, con funzioni di vigilanza del mercato e della sua corretta applicazione. Gli Stati membri possono decidere se creare un'autorità di controllo per l'IA *ad hoc* o affidare le relative funzioni e responsabilità ad un'autorità indipendente già esistente[5]. Ad ogni modo, come

[4] Ci si riferisce, nello specifico, alle procedure relative alla valutazione di conformità (*compliance assessment*) e alle valutazioni di impatto sui diritti fondamentali (FRIA) derivante dall'utilizzo dei sistemi di IA. Per commenti preliminari sulle valutazioni di conformità, si veda J. Mökander, M. Axente, F. Casolari, L. Floridi, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, in *Minds&Machines*, 2022, p. 241 ss.

[5] Vale la pena anticipare che alcuni Stati membri hanno già provveduto a individuare le autorità di vigilanza, secondo diverse sensibilità: la Spagna ha costituito *ex novo* un'Agenzia apposita (AESIA), l'Olanda invece ha indicato il Garante per la *privacy*, mentre in Austria la scelta è ricaduta sull'Autorità competente in materia di telecomunicazioni.

specificato al paragrafo 3 della medesima disposizione, è necessario che le autorità nazionali competenti «dispongano di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti».

Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Tuttavia, le autorità dovranno agire «in modo *indipendente, imparziale e senza pregiudizi*, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti nell'applicazione e attuazione del regolamento [corsivo aggiunto]»[6]. Nell'economia complessiva del regolamento, il rinvio a tali requisiti è coerente con i compiti affidati alle autorità che, pur non essendo organi giurisdizionali, avranno anche poteri investigativi e correttivi. In aggiunta, il carattere imparziale delle autorità di vigilanza è legato al principale obiettivo dell'*AI Act*, ovvero all'esigenza di promuovere un elevato livello di tutela dei diritti fondamentali che saranno profondamente e trasversalmente toccati dai sistemi di intelligenza artificiale[7].

Sul piano operativo, all'art. 74 dell'*AI Act*, il legislatore ha avuto premura di articolare i poteri delle autorità di vigilanza create *ex novo* rinviando esplicitamente al sistema istituito dal reg. 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti[8]. Non potendo qui approfondire in modo puntuale quanto previsto da detto regolamento, basti dire che le autorità nazionali prescelte per monitorare l'immissione nel mercato dei sistemi di IA avranno sostanzialmente due tipologie di funzioni.

[6] Regolamento 2024/1689, art. 70 (1).

[7] Sul punto merita sottolineare che in Italia il confronto è particolarmente serrato proprio in riferimento al tema dell'indipendenza dell'autorità. Da una parte, infatti, il governo avrebbe l'intenzione di affidare i compiti di vigilanza all'Agenzia per l'Italia digitale e all'Agenzia per la cybersicurezza; due agenzie che, come sostenuto da più parti, difetterebbero del requisito cruciale dell'indipendenza. Dall'altra, il Garante Privacy ha rivendicato il proprio ruolo privilegiato nell'attuazione dell'*AI Act*, «in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza. […] Il Garante possiede infatti, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione del Regolamento coerente con l'obiettivo di garanzia di un livello elevato di tutela dei diritti fondamentali nel ricorso all'IA, sancito dall'art. 1, p. 1». Si veda, Garante per la protezione dei dati personali, Segnalazione al Parlamento e al Governo sull'Autorità per l'Intelligenza Artificiale del 25 marzo 2024.

[8] Regolamento 2019/1020, spec. artt. 11 e 14.

La prima funzione sarà essenzialmente di supporto dal momento che le autorità potranno fornire orientamenti e consulenza sull'attuazione del regolamento, in particolare in favore delle PMI, comprese le *start-up*, tenendo conto, a seconda dei casi, degli orientamenti e della consulenza del Comitato scientifico e della Commissione[9].

La seconda funzione, ben più articolata, comprende invece la pura vigilanza. Sebbene, infatti, la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici in quanto non categorizzati come ad alto rischio, le autorità di vigilanza del mercato potranno adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conformemente al regolamento[10]. Le autorità potranno quindi chiedere ai fornitori informazioni e accedere alla documentazione, sollecitare l'adozione di misure correttive e il ritiro del sistema dal mercato qualora non conforme a quanto previsto dal regolamento.

Fatti salvi i poteri di controllo di propria iniziativa, ai sensi dell'art. 73 dell'*AI Act* l'adozione delle menzionate misure potrebbe avvenire a seguito della ricezione di segnalazioni relative a gravi incidenti da parte dei fornitori di IA, di cui l'autorità di vigilanza dovrà informare gli organismi pubblici nazionali nonché la Commissione sulla base di quanto già previsto dagli artt. 19 e 20 del reg. 2019/1020[11]. Oppure, come stabilito dall'art. 85, «qualsiasi persona fisica o giuridica» che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del reg. 2024/1689 potrà presentare all'autorità di vigilanza un reclamo motivato. Questa opportunità, vale la pena sottolinearlo, rappresenta un elemento estremamente positivo poiché, inserito per volontà del Parlamento europeo, si aggiunge ai rimedi giurisdizionali e amministrativi volti a dare concretezza al diritto ad un ricorso effettivo stabilito all'art. 47 della Carta dei diritti fondamentali[12]. Ciononostante, vista le penuria di dettagli che caratterizza tanto l'art. 85 quanto il reg. 2019/1020 in ordine alla procedura sui reclami, è immaginabile che spetterà agli Stati

[9] Per approfondimenti, si rinvia al contributo di F. Ferri, *op. cit*.

[10] Regolamento 2024/1689, artt. 79 e 80.

[11] Regolamento 2024/1689, art. 73, parr. 9-12.

[12] Per commenti sulla portata di tale diritto, si veda D. Domenicucci, F. Filpo, *Art. 47*, in R. Mastroianni, O. Pollicino, S. Allegrazza, F. Pappalardo, O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 864 ss.; G. D'Avino, *Il diritto alla tutela giurisdizionale effettiva nell'art. 47 par. 1 della Carta dei diritti fondamentali dell'UE*, in A. Di Stasi (a cura di), *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale della Carta*, Napoli, 2019, p. 151 ss.; M. Bonelli, M. Eliantonio, G. Gentile (eds.), *Article 47 of the EU Charter and Effective Judicial Protection, The Court of Justice's Perspective*, Oxford, 2022.

membri stabilire le modalità di raccordo con il sistema di tutela giurisdizionale nazionale, una volta designate le autorità competenti.

Qualora le misure correttive di cui sopra non siano sufficienti, l'art. 99 introduce la possibilità per le autorità di vigilanza di adottare sanzioni pecuniarie e altre misure di esecuzione, inclusi avvertimenti e misure di natura non pecuniaria, applicabili in caso di violazione del regolamento da parte degli operatori. Mentre non si ritrovano specifiche circa la portata delle potenziali misure non pecuniarie, lasciando così liberi gli Stati di stabilire le regole di dettaglio, il regolamento è più stringente rispetto alle condizioni affinché le autorità possano infliggere sanzioni pecuniarie di carattere amministrativo. Infatti, all'art. 99 (7), è espressamente richiesto di tenere in debita considerazione tutte le circostanze pertinenti della situazione specifica e, nel caso, di ulteriori criteri ivi menzionati. Quanto all'importo delle sanzioni pecuniarie, l'*AI Act* prevede dei massimali fissati sulla base di due riferimenti alternativi: un ammontare predeterminato oppure una percentuale del fatturato annuo globale nell'anno finanziario precedente. Si tratterebbe, quantitativamente, di € 35 milioni o del 7% del fatturato per violazioni circa l'applicazione di sistemi di IA vietati; € 15 milioni o il 3% del fatturato per violazioni degli obblighi previsti dal regolamento; e, infine, € 7,5 milioni o l'1,5% del fatturato per la comunicazione di informazioni errate[13]. Tenuto conto di queste soglie, gli Stati membri dovranno stabilire sanzioni efficaci, proporzionate e dissuasive, comprese le sanzioni amministrative, e comunicarle alla Commissione[14]. In aggiunta, spetterà sempre agli Stati introdurre delle regole che definiscano in quale misura potranno essere inflitte sanzioni ad autorità pubbliche e organismi pubblici nazionali in caso di violazione degli obblighi previsti dal reg. 2024/1689[15].

In ogni caso, l'esercizio da parte dell'autorità di vigilanza del mercato dei poteri sanzionatori dovrà essere soggetto alle garanzie procedurali previste dal diritto dell'Unione e da quello nazionale, inclusi il diritto ad un ricorso giurisdizionale effettivo e il giusto processo[16]. Ci si può dunque

[13] Regolamento 2024/1689, art. 99, parr. 3-5. Occorre segnalare che, rispetto alla proposta della Commissione, l'accordo raggiunto tra Parlamento e Consiglio ha introdotto massimali più proporzionati alle sanzioni amministrative per le PMI e le *start-up* in caso di violazione delle disposizioni dell'*AI Act*. Si veda, Regolamento 2024/1689, art. 99, par. 6.

[14] Regolamento 2024/1689, art. 71.

[15] Regolamento 2024/1689, art. 99, par. 8. Occorre qui precisare che i fornitori di modelli di IA per finalità generali saranno sanzionabili direttamente dalla Commissione, Regolamento 2024/1689, art. 101. Per approfondimenti, si rinvia al contributo di F. Ferri, *op. cit*.

[16] Regolamento 2024/1689, art. 99, par. 10. Per approfondimenti sul tema in generale,

immaginare che i provvedimenti adottati dalle autorità di vigilanza possano essere sottoposti al sindacato delle Corti nazionali (e, nel caso, della Corte di giustizia tramite un rinvio pregiudiziale) nel rispetto, nuovamente, dell'art. 47 della Carta. Preme comunque precisare che la funzione sanzionatoria non è demandata in via esclusiva alle autorità di vigilanza che dovranno controllare sulla corretta applicazione del regolamento. Infatti, il paragrafo 9 dell'art. 99 lascia liberi gli Stati di prevedere che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi, secondo il proprio ordinamento giuridico nazionale. Dunque, in linea con l'autonomia procedurale degli Stati membri, non solo la dimensione organizzativa delle autorità di vigilanza ma anche la distribuzione dei poteri rispetto all'imposizione di eventuali sanzioni in caso di violazioni dell'*AI Act* si configura sotto un profilo scarsamente armonizzato a livello sovranazionale, se non rispetto a dei criteri minimi, e sostanzialmente affidato alle normative nazionali.

3. *La vigilanza sull'applicazione dell'*AI Act *da parte dell'Unione: il Garante europeo per la protezione dei dati*

Per quanto riguarda l'Unione europea, destinataria anch'essa delle medesime procedure di controllo dei sistemi di IA successive all'immissione nel mercato, il regolamento stabilisce che il Garante europeo per la protezione dei dati (di seguito: Garante europeo o GEPD)[17] venga designato quale autorità di vigilanza del mercato competente per le istituzioni, organi e organismi dell'Unione[18]. Rispetto dunque alla definizione di «autorità di vigilanza del mercato» stabilita all'art. 3 (4) del reg. 2019/1020[19] applicabile negli Stati

si rinvia a W. Kotschy, *Article 78 Right to an effective judicial remedy against a supervisory authority*, in C. Kuner et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, 2020, p. 1125 ss.; G. Di Federico, *La riforma del procedimento comunitario antitrust e i diritti di difesa*, Napoli, 2008.

[17] Istituito nel 2004 e con sede a Bruxelles, il Garante europeo della protezione dei dati (GEPD) è l'autorità di controllo indipendente della protezione dei dati dell'Unione europea. I compiti del Garante sono esaustivamente elencati nel capitolo VI del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[18] Regolamento 2024/1689, art. 70, par. 9. Ad eccezione, si badi bene, della Corte di giustizia, come specificato all'art. 74, par. 9.

[19] Ai sensi dell'art. 3 (4) del regolamento 2019/1020, cit., «l'autorità di vigilanza del mer-

membri, il «mercato» in cui il GEPD va ad esercitare il ruolo di autorità di vigilanza non è limitato ad un territorio fisico, ma si estende ad *ogni* spazio in cui il sistema di IA viene fornito da parte delle istituzioni, degli organismi e degli organi dell'Unione che rientrano nell'ambito di applicazione dell'*AI Act*[20].

Quanto ai suoi compiti, il Garante europeo è chiamato a monitorare l'applicazione del reg. 2024/1689 e intervenire con gli strumenti attribuiti alle autorità di vigilanza nazionali. Per analogia, anche il Garante europeo potrà quindi adottare misure provvisorie per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo. Il Garante avrà poi la possibilità di acquisire i reclami dei singoli (nella veste di persone fisiche o giuridiche) previsti dall'art. 85 in caso di violazioni dell'*IA Act* da parte delle istituzioni e degli organismi dell'Unione, senza pregiudicare gli altri possibili rimedi amministrativi o giudiziari, quali ad esempio quelli avviati di fronte alla Corte di giustizia. Su questo aspetto, occorre però puntualizzare che si tratta, per l'appunto, di un'interpretazione per analogia, dal momento che l'*AI Act* non va a disciplinare specificamente la questione dei reclami da poter presentare al Garante europeo. Pertanto, sarà necessario procedere tramite un'operazione di integrazione normativa con atti già esistenti, ovvero il noto reg. 2016/679 (RGPD)[21] e il reg. 2018/1725[22]. Infatti, solo una lettura congiunta di questi atti può chiarire ulteriormente le competenze e le opzioni di intervento di detta autorità in materia di intelligenza artificiale. A titolo esemplificativo, ciò dovrebbe implicare che, nel silenzio dell'*AI Act*, venga esteso il diritto ad un ricorso giurisdizionale effettivo nei confronti del Garante europeo previsto all'art. 58 del reg. 2018/1725[23] anche qualora questo non abbia dato seguito ad un reclamo relativo all'applicazio-

cato è un'autorità designata da uno Stato membro a norma dell'articolo 10 quale responsabile della vigilanza del mercato nel territorio di tale Stato membro».

[20] EDPS, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, punti 38 e 39.

[21] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

[22] Regolamento (UE) 2018/1725, cit.

[23] Ai sensi dell'art. 58, par. 5, del regolamento 2018/1725, cit., «L'esercizio da parte del Garante europeo della protezione dei dati dei poteri attribuitigli dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione».

ne dell'*AI Act* o non abbia informato circa lo stato del medesimo.

Il regolamento è invece decisamente più esplicito in ordine al potere del GEPD di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione in caso di violazione delle norme previste dall'*IA Act*; un eventuale tesoretto, quello derivante dalle sanzioni, che andrà a contribuire al bilancio generale dell'Unione. L'art. 100 va a dettagliare tale potere, specificando le condizioni che dovranno essere rispettate per poter procedere con l'inflizione delle sanzioni.

Rispetto al meccanismo sanzionatorio previsto per i soggetti privati ai sensi dell'art. 99 illustrato nel paragrafo precedente, si prevede esplicitamente la sola possibilità di infliggere misure pecuniarie, peraltro particolarmente esigue rispetto a quelle imposte nei confronti degli operatori privati. Infatti, per le istituzioni dell'Unione la non conformità al divieto delle pratiche di IA di cui all'art. 5, ovvero quelle vietate, sarà soggetta a sanzioni amministrative pecuniarie fino a €1 milione e mezzo; la non conformità del sistema di IA ai requisiti o agli altri obblighi previsti dal regolamento, sarà soggetta a sanzioni fino a €750 mila. In queste circostanze, tenuto conto del pieno diritto di difesa delle parti, il Garante dovrà concedere alle istituzioni/organi dell'Unione l'opportunità di esprimersi in merito all'eventuale violazione, valutando poi la sanzione da infliggere sulla base dei criteri di cui all'art. 100, par. 1. A differenza della successiva disposizione, relativa alle sanzioni che la Commissione può adottare nei confronti di fornitori di sistemi di IA con finalità generale[24], l'art. 100 non prevede esplicitamente la possibilità per la Corte di giustizia di esaminare le sanzioni applicate dal Garante. Tuttavia, anche in questo caso, può venire in soccorso la lettura congiunta di quest'ultima disposizione dell'*AI Act* con l'art. 64 del reg. 2018/1725 che riconosce tale competenza alla Corte di giustizia, la quale, in caso di ricorso, potrebbe estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.

Ad ogni modo, non è da escludere che i poteri investigativi e di sorveglianza in capo al Garante europeo saranno ulteriormente specificati nelle future misure di esecuzione al fine di rendere operative ed efficaci le disposizioni dell'*AI Act*.

[24] Regolamento 2024/1689, art. 101, par. 5. Per approfondimenti, si rinvia al contributo di F. Ferri, *op. cit*.

4. *Sistema di vigilanza e strumenti di cooperazione tra autorità*

La struttura di *governance* appena illustrata denota un tipo di vigilanza potenzialmente frammentata ed incentrata su interventi circoscritti al territorio dei rispettivi Stati membri e, nel caso del Garante europeo, alle attività svolte dalle istituzioni dell'Unione. Ciononostante, nello spazio dinamico ed interconnesso in cui si muovono i sistemi di intelligenza artificiale, le singole autorità di vigilanza potrebbero trovarsi ad interagire reciprocamente. Pertanto, occorre approfondire gli strumenti che potrebbero supportare una maggior cooperazione tra le autorità di vigilanza tanto a livello nazionale quanto a livello sovranazionale per garantire la piena applicazione del regolamento.

Nello specifico, due sono gli scenari di interazione su cui vale la pena soffermarsi. Il primo scenario è riconducibile al rapporto tra autorità di vigilanza appartenenti al medesimo Stato membro che potrebbero vantare una competenza in ordine all'applicazione dell'*AI Act* (par. 4.1). Il secondo scenario riguarda, invece, l'interazione tra autorità di vigilanza operanti in diversi Stati membri o con il Garante europeo qualora, ad esempio, talune categorie di sistemi di IA presentino un rischio grave in due o più Stati membri oppure a livello UE (par. 4.2).

4.1. Segue*: a livello intrastatale*

Come detto, agli Stati membri è garantita la discrezionalità di indicare una o più autorità di vigilanza del mercato che provvedano a dare corretta applicazione all'*AI Act*. Tuttavia, il regolamento prevede tre eccezioni rispetto alla determinazione delle autorità competenti in ordine ai sistemi di IA ad alto rischio. La prima eccezione è indicata all'art. 74, par. 3, secondo cui, salvo diversa e motivata decisione adottata a livello nazionale, l'autorità di vigilanza del mercato per i sistemi collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, sarà quella già designata a norma di tali atti giuridici[25]. In secondo luogo, per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari e creditizi, l'autorità di vigilanza del mercato sarà quella responsabile della vigilanza finanziaria (art. 74, par. 6). La terza eccezione, prevista

[25] Il regolamento si riferisce, nello specifico, alla normativa relativa ai prodotti già sottoposti a controlli nel quadro del mercato interno.

all'art. 74, par. 8, riguarda i sistemi utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e tutela dei processi democratici nonché i sistemi di IA ad alto rischio elencati nell'allegato III[26]: in questi casi, gli Stati membri dovranno designare come autorità di vigilanza del mercato le autorità di controllo competenti per la protezione dei dati a norma del reg. 2016/679 e della dir. 2016/680 (cd. direttiva polizia)[27].

Le riserve di competenza espressamente previste dal regolamento sono finalizzate ad evitare che le attività di vigilanza pregiudichino la capacità delle autorità già esistenti di svolgere i loro compiti secondo quanto richiesto dalla normativa dell'Unione. In particolare, l'attribuzione di taluni poteri di vigilanza alle autorità nazionali per la protezione dei dati personali è motivata dalla stretta interrelazione tra IA e protezione dei dati; un legame che si rinviene anche nella competenza che dette autorità hanno acquisito rispetto al processo decisionale automatizzato[28]. In effetti, l'area di tutela relativa ai dati personali è certamente una delle più interessate dalla diffusione e pervasività dei sistemi di intelligenza artificiale perché l'elaborazione, l'analisi e il trattamento di grandi quantitativi di dati sono alla base del funzionamento dell'intelligenza artificiale. Tuttavia, i diritti fondamentali che il reg. 2024/1689 intende tutelare sono riconducibili ad un insieme più ampio, a seconda della tecnologia e dell'ambito di utilizzo. Per questo, a differenza di

[26] Nel dettaglio, la disposizione fa riferimento all'utilizzo dei sistemi di IA per la raccolta di dati biometrici (Allegato III, punto 1) e ai sistemi ad alto rischio previsti nell'Allegato III, punti 6, 7 e 8. Da notare che le autorità per la protezione dei dati dovrebbero auspicabilmente presentare alla Commissione una relazione annuale sull'uso dei sistemi di identificazione biometrica 'in tempo reale'; un auspicio che, tuttavia, è previsto esclusivamente nel considerando n. 36 ma non si ritrova nel testo del regolamento.

[27] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[28] Regolamento 2016/679, cit., art. 22. Per approfondimenti, F. Ufert, *AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?*, in *EP*, n. 5, 2020, p. 1087 ss.; G. Sartor, F. Lagioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, *European Parliament Study*, 2020; J. Andraško, M. Mesarčík, O. Hamuľák, *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, in *AI & Soc*, 2021, p. 623 ss.; G. Contaldi, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, p. 207 ss.; T. Frosini, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, n. 1, 2022, p. 273 ss.

quanto auspicato dal Garante europeo nel parere emesso nel 2021[29], è stata confermata la linea avanzata nella proposta iniziale della Commissione di non imporre agli Stati membri la designazione delle autorità di protezione di dati quali autorità competenti rispetto all'applicazione generale dell'*AI Act*. Invece, la competenza in materia di vigilanza sull'applicazione del regolamento sull'IA spetterà, come regola generale, alle autorità di controllo da esso istituite o designate appositamente e soltanto in via d'eccezione alle altre autorità nazionali.

La potenziale attribuzione del potere di vigilanza a diverse autorità comporterà la ricerca di uno stringente coordinamento tra queste al fine di garantire l'effettiva ed efficace applicazione del regolamento sul piano nazionale. La portata dell'interazione tra autorità di controllo afferenti a distinti ambiti di intervento è stata affrontata (per la prima volta) dalla Corte di giustizia nella recente pronuncia relativa al caso *Meta Platforms e a.*, del 4 luglio 2023[30]. Nel caso di specie, si lamentava il fatto che l'interpretazione, da parte delle autorità antitrust, delle disposizioni del RGPD al fine di constatare una violazione del diritto della concorrenza avrebbe determinato un potenziale *vulnus* alle competenze delle autorità per la *privacy*. Ebbene, qui i giudici hanno riconosciuto alle autorità amministrative degli Stati membri la possibilità di esercitare una competenza condivisa, purché non sostitutiva[31], desumendo una serie di obblighi di collaborazione e di coordinamento tra dette autorità direttamente dal principio di leale collaborazione, previsto dall'art. 4, par. 3, TUE[32]. Pare pacifico sostenere che, se questo ragionamento vale per autorità di controllo con compiti e obiettivi distinti ma che ad un certo punto possono convergere, a maggior ragione le autorità amministrative espressamente titolate ad intervenire per vigilare sull'attuazione dell'*AI*

[29] EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), punto 47.

[30] In dottrina P. Manzini, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, n. 10, 2023, p. 196 ss.; I. Graef, *Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment*, in *MJECL*, 2023, p. 325 ss.; P. G. Picht, *CJEU on Facebook: GDPR Processing Justifications and Application Competence*, in *Gewerblicher Rechtsschutz und Urheberrecht*, n. 16, 2023, p. 1169 ss., M. Previatello, *L'obbligo di leale cooperazione tra autorità nazionali garanti della concorrenza e autorità di controllo istituite dal RGPD nella sentenza Meta Platforms e a.*, in *Quaderni AISDUE*, n. 1, 2024, p. 1 ss.

[31] Corte giust. 4 luglio 2023, C-252/21, *Meta Platforms e a.*, punto 44 ss. Sul rapporto tra diritto antitrust e IA, si veda P. Manzini, *Intelligenza artificiale e diritto della concorrenza, in: XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 422 ss.

[32] *Meta Platforms e a.*, sopra citata, punto 53.

Act dovranno cooperare tra loro al fine di garantire, da un lato, l'effettiva applicazione del diritto settoriale e, dall'altro, la coerenza del sistema di protezione istituito dal regolamento sull'IA[33].

Questa esigenza è pure desumibile dalla risalente giurisprudenza della Corte di giustizia, secondo cui le autorità amministrative degli Stati membri devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura necessaria per assicurare l'adempimento degli obblighi risultanti dagli atti adottati dalle istituzioni, nonché evitare di adottare qualsiasi misura che potrebbe compromettere il raggiungimento degli obiettivi dell'Unione[34]. Ad ogni modo, dal momento che questo aspetto relativo alla cooperazione tra autorità nazionali non è disciplinato esaustivamente dall'*AI Act*, è probabile – oltre che auspicabile – che in futuro sia richiesto ai giudici di Lussemburgo di pronunciarsi in modo tale da escludere, o quantomeno mitigare, il rischio di divergenze tra le diverse autorità nazionali in merito al controllo sull'attuazione del regolamento.

4.2. Segue*: a livello interstatale e sovranazionale*

La regolamentazione introdotta dall'*AI Act* disciplina la cooperazione tra le autorità nazionali di controllo interessate a livello interstatale e la cooperazione di tali autorità con il Comitato europeo per l'intelligenza artificiale[35] e l'Ufficio per l'IA, incaricati di sorvegliare sulla corretta applicazione del regolamento nei vari Stati membri e di elaborare linee guida in materia,

[33] Sul principio di leale cooperazione tra gli Stati membri, si veda P. De Pasquale, *Commento all'art. 4 TUE*, in A. Tizzano (a cura di), *Trattati dell'Unione europea*, II ed., Milano, 2014, spec. p. 28 ss.; M. Klamert, *Article 4 TEU*, in M. Kellerbauer et al. (eds.), *The EU Treaties and the Charter of Fundamental Rights — A Commentary*, Oxford, 2019, p. 35 ss.; F. Casolari, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020.

[34] Corte giust. 7 novembre 2013, C-518/11, *UPC Nederland*, punto 59; 1° agosto 2022, C-14/21 e C-15/21, *Sea Watch*, punto 156.

[35] Come previsto dal considerando n. 149 dell'*AI Act*, al fine di facilitare l'attuazione agevole, efficace e armonizzata delle norme stabilite nell'*AI Act* viene istituito un Comitato europeo per l'intelligenza artificiale finalizzato a «riflettere i vari interessi dell'ecosistema dell'IA». A tal fine, *ex* art. 65, il Comitato sarà composto da un rappresentante per Stato membro, designato per tre anni e rinnovabile una sola volta. Per offrire una certa flessibilità agli Stati membri nella designazione dei loro rappresentanti all'interno del Comitato, che pur dovranno garantire obiettività e imparzialità, tali rappresentanti potranno appartenere a entità pubbliche dotate delle competenze e dei poteri pertinenti per facilitare il coordinamento e la coerenza a livello nazionale e contribuire all'adempimento dei compiti del comitato.

specialmente in relazione ai modelli fondativi e GPAI[36]. In particolare, l'art. 74, par. 11, del regolamento prevede che le autorità di vigilanza del mercato degli Stati membri e la Commissione propongano attività congiunte al fine di promuovere la conformità, sensibilizzare e fornire orientamenti in relazione al reg. 2024/1689 riguardo a specifiche categorie di sistemi di IA ad alto rischio che presentino un rischio grave in due o più Stati membri. Queste attività di natura congiunta dovrebbero basarsi sulla procedura prevista all'art. 9 del reg. 2019/1020 e sotto il coordinamento dell'Ufficio per l'IA[37].

Oltre che a raccordarsi sulle *best practices*, obiettivo questo dettato dall'impostazione generale dell'*AI Act* di prevenire più che reprimere eventuali pratiche, il regolamento prevede anche la possibilità di attivare indagini congiunte tra autorità di vigilanza. Ai sensi dell'art. 79, par. 3, del regolamento, se l'autorità di vigilanza di uno Stato membro ritiene che la violazione non sia limitata al suo territorio nazionale ma possa avere un impatto transnazionale, dovrà informare la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni richieste al fornitore o all'utilizzatore del sistema di IA. In tali casi, dovrebbe dunque applicarsi *mutatis mutandis* la procedura relativa all'assistenza reciproca e allo scambio di informazioni nei casi transfrontalieri di cui alle disposizioni del capo VI del reg. 2019/1020. In aggiunta, il reg. 2024/1689 prevede che qualsiasi autorità di vigilanza del mercato chieda assistenza all'Ufficio per l'IA qualora non sia in grado di concludere un'indagine su un sistema ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali su cui è costruito il sistema sottoposto ad indagine.

Degno di nota è, infine, l'art. 81 che conferma il ruolo predominante della Commissione all'interno del disegno complessivo del regolamento[38], attribuendole una serie di poteri che le permettono di prevalere sulle decisioni delle autorità nazionali. Infatti, è qui previsto che, qualora l'autorità di vigilanza del mercato di uno Stato membro sollevi obiezioni contro una misura adottata da un'altra autorità di vigilanza del mercato, o la Commissione ritenga che la misura sia contraria al diritto UE, quest'ultima consulterà l'autorità di vigilanza interessata e l'operatore, e valuterà se la misura nazionale è giustificata.

[36] Per approfondimenti, si rinvia al contributo di F. Ferri, *op. cit*.

[37] Peraltro, in riferimento alle presunte violazioni da parte di fornitori di GPAI, va detto che l'Ufficio per l'*IA*, pur esclusivamente competente, si attenderà una stretta collaborazione, in termini di segnalazioni e trasferimento di informazioni, da parte delle autorità di vigilanza nazionali.

[38] Per approfondimenti, si rinvia al contributo di F. Ferri, *op. cit*.

Questa impostazione riflette certamente l'esigenza di garantire che le autorità nazionali di vigilanza operino in modo coordinato, informato e congiunto nel momento in cui si ritenga che si possa verificare un utilizzo improprio dei sistemi di IA con impatto non solo a livello nazionale ma anche sovranazionale. Sebbene il sistema di vigilanza transnazionale figurato nell'*AI Act* appaia quindi apprezzabile grazie al rinvio a strumenti di mutua assistenza, esso è al contempo "zoppicante". In effetti, a parere di chi scrive, le disposizioni relative al sistema di vigilanza sono estremamente vaghe e, pur rinviando al più generale reg. 2019/1020, tradiscono un carattere più programmatico che precettivo. Questo approccio conferma il compromesso raggiunto nella costruzione di un meccanismo di vigilanza che, ben lungi dall'avere un carattere decisamente sovranazionale, si è assestato sulle esigenze nazionali di controllo. A conferma di ciò, occorre sottolineare il cambiamento che caratterizza la versione finale dell'*AI Act* rispetto alla proposta della Commissione. Infatti, il Comitato europeo per l'IA doveva essere composto dalle autorità nazionali di vigilanza, compreso evidentemente il Garante europeo: in altre parole, in quanto autorità di sintesi delle singole autorità di vigilanza, il Comitato si sarebbe auto promosso ad autorità indipendente europea. Tuttavia, questo impianto è stato mitigato a seguito dell'accordo raggiunto nel trilogo, attribuendo la funzione di *trait-d'union* rispetto alla cooperazione amministrativa al sottogruppo permanente per la vigilanza del mercato (ADCO) per l'*AI Act*[39], sotto il coordinamento della Commissione europea che mantiene ben saldo il potere regolatorio. Resta da chiedersi fino a che punto il Comitato, che potrà sostanzialmente adottare solo atti di *soft law*, potrà garantire una supervisione (seppur debole) sull'applicazione uniforme del regolamento. Ciò, tenuto poi conto che il Garante europeo parteciperà al Comitato solamente in qualità di osservatore, smorzando così il carattere sovranazionale del coordinamento.

A fronte di ciò, il rischio che le autorità degli Stati membri possano rivendicare la competenza, determinando una frammentazione dell'applicazione ed eventualmente l'adozione di decisioni contrastanti, non è trascurabile, special-

[39] Ai sensi dell'art. 65, par. 6, dell'*AI Act*, il Comitato sarà composto da due sottogruppi permanenti per fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni relative. Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per l'*AI Act* ai sensi dell'art. del regolamento (UE) 2019/1020. In conformità poi dell'art. 33 di quest'ultimo regolamento, la Commissione dovrebbe sostenere le attività del sottogruppo permanente per la vigilanza del mercato effettuando valutazioni o studi di mercato, in particolare al fine di individuare quelli che richiedono un coordinamento specifico e urgente tra le autorità di vigilanza del mercato.

mente per i destinatari di indagini e sanzioni amministrative. Sarà pertanto necessario che le manovre delle autorità si fondino, di nuovo, sul principio di leale collaborazione previsto dall'art. 4, par. 3, TUE, auspicabilmente attingendo ai requisiti e alle modalità di cooperazione tra autorità nazionali già individuati dalla Corte di giustizia nel noto caso *Facebook Ireland e a*.[40]. In quell'occasione, infatti, i giudici di Lussemburgo avevano confermato la ripartizione delle competenze tra le autorità di vigilanza di diversi Stati membri per preservare il cd. "*one-stop shop mechanism*"[41], sottolineando l'importanza di una cooperazione non solo efficace (come espressamente previsto dal RGPD) ma anche leale tra di loro. Ciò, per tornare al reg. 2024/1689, al fine di garantire un'attuazione coerente e omogenea della normativa oltreché una maggiore prevedibilità per i soggetti coinvolti nella fornitura e nell'utilizzo di sistemi di IA[42]. Vista la portata dell'*AI Act* e l'impatto della sua applicazione, è certo che la Corte di giustizia sarà in futuro chiamata a pronunciarsi anche su questi aspetti.

5. *Riflessioni conclusive*

Il sistema di *governance* relativo alla vigilanza sull'applicazione dell'*AI Act* è particolarmente complesso, tentando di porsi come un correttivo di natura complementare e ancillare rispetto ai meccanismi di tutela *ex ante*. Non solo. Il sistema illustrato pare fortemente orientato a tutelare, tanto sul piano organizzativo quanto funzionale, le esigenze di controllo sull'IA degli Stati membri. Questo è confermato, in particolare, dal tenore delle disposizioni sulle autorità di vigilanza nazionali che garantiscono ampia discrezionalità agli Stati nella designazione di dette autorità.

Nel quadro normativo dell'Unione, questo secondo punto è particolarmente dirimente. Infatti, come si è avuto modo di sottolineare, sul piano costituzionale è certamente rilevante il rinvio ad uno dei principi cardine del

[40] Corte giust. 15 giugno 2021, C-645/19. Per commenti, si veda S. BRETTAUER, *Extended powers for other supervisory authorities concerned in the case of cross-border data processing: Facebook Ireland*, in *CMLR*, n. 2, 2022, p. 1543 ss.; L. CHEMLALI, *The competence of non-lead supervisory authority under the EU GDPR'S one-stop-shop mechanism: CJEU judgment in Facebook and Others (C-645/19)*, in *Journal of Media Law*, n. 2, 2022, p. 208 ss.

[41] Previsto dall'art. 60 del RGPD, tale meccanismo (denominato in italiano 'sportello unico') è stato poi incorporato e dettagliato nelle linee guida adottate il 28 marzo 2023 dal Garante europeo sull'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento.

[42] *Facebook Ireland e a*., sopra citata, punti 53, 60, 63 e 72.

diritto UE, ovvero il principio di leale cooperazione che, come noto, non si esaurisce nella reciproca assistenza per l'adempimento dei compiti derivanti dai trattati ma anche nell'astensione da qualsiasi misura che rischi di mettere in pericolo la realizzazione degli obiettivi dell'Unione. Richiedere, dunque, che le autorità di vigilanza si coordinino, sia sul piano interno che su quello sovranazionale, per garantire l'effettività del regolamento sull'IA rappresenta certamente un obbligo di leale cooperazione a cui pure le autorità amministrative devono conformarsi nel caso di specie. Al contempo, però, non può sfuggire l'assenza di soggetto indipendente che garantisca un coordinamento effettivo e stringente tra le autorità di vigilanza, compreso il Garante europeo per quanto attiene le istituzioni dell'Unione. Infatti, per come configurato nel reg. 2024/1689, il sottogruppo per la vigilanza del mercato del Comitato europeo per l'IA rappresenta una semplice piattaforma di cooperazione e scambio tra le autorità nazionali senza determinanti poteri di armonizzazione. In assenza di un sistema di raccordo indipendente a livello sovranazionale, sarà la Commissione europea, e dunque un'istituzione politica nonché l'esecutivo dell'Unione, ad assumere il ruolo di "super controllore" del sistema di vigilanza, potendo valutare, in caso di dubbi, se le misure adottate dalle autorità nazionali rispetto ai sistemi di IA immessi nel mercato siano giustificate.

In conclusione, per come attualmente configurata, nonostante la rilevanza delle misure sanzionatorie e la possibilità per le autorità di richiedere il ritiro dal mercato o il richiamo dei prodotti, la disciplina complessiva in materia di vigilanza non appare del tutto sufficiente a garantire un'applicazione efficace. L'esperienza del RGPD mostra che un eccessivo affidamento sull'*enforcement* delle autorità nazionali espone al rischio di difformità applicative, a causa delle notevoli divergenze di risorse e prassi di intervento nei diversi Stati membri[43]. Com'è usuale in campo tecnologico, poi, si pone il problema di possibili difformità nei criteri di valutazione degli *standard* tecnici, che sarà tanto più pregnante in un settore, quello dell'IA, caratterizzato da un elevato numero di attori e di *standard* diversi. Il successo dell'*AI Act* si misurerà, dunque, anche sulla capacità di vigilanza da parte delle autorità ma anche in quella delle istituzioni dell'Unione – *in primis* Commissione europea e Corte di giustizia – di lavorare per individuare dei profili di cooperazione stringente tra le singole autorità di controllo, permettendo a queste di stare al passo con lo sviluppo estremamente celere dei sistemi di IA.

[43] G. De Minico, *Autorità indipendenti e algoritmi: una famiglia disfunzionale*, in *Osservatorio sulle fonti*, n. 2, 2021, p. 981 ss.

Abstract (ita)

Il complessivo sistema di vigilanza previsto dal regolamento 2024/1689 sull'intelligenza artificiale si articola su un doppio livello, quello sovranazionale e quello nazionale, ed è finalizzato a completare il meccanismo di controllo e verifica precedente all'immissione nel mercato dei sistemi di intelligenza artificiale. Nello specifico, il regolamento prevede che gli Stati membri designino una o più autorità nazionali competenti, con funzioni di vigilanza del mercato e della sua corretta applicazione, con possibilità di esercitare poteri sanzionatori. D'altro canto, il Garante europeo per la protezione dei dati è stato designato quale autorità di vigilanza del mercato competente per i sistemi di IA utilizzati da istituzioni, organi e organismi dell'Unione. Questa impostazione di *governance*, frammentata e foriera di tensioni, richiederà un importante sforzo di coordinamento, sia sul piano interno che su quello sovranazionale, quale espressione del principio di leale cooperazione previsto dall'art. 4, par. 3, TUE e ribadito a più riprese dalla recente giurisprudenza della Corte di giustizia in materia di vigilanza.

Abstract (eng)

The overall supervisory system provided for by the Regulation 2024/1689 on Artificial Intelligence is divided into two levels, supranational and national, and is aimed at completing the control and verification mechanism prior to the placing of artificial intelligence systems on the market. Specifically, the Regulation provides that Member States shall designate one or more competent national authorities, with functions of market surveillance and its proper application, with the possibility of exercising sanctioning powers. On the other hand, the European Data Protection Supervisor has been designated as the competent market surveillance authority for AI systems used by Union institutions, bodies, offices and agencies. This approach to *governance*, which is fragmented and fraught with tensions, will require a major effort of coordination, both internally and supranationally, as an expression of the principle of sincere cooperation provided for in Art. 4(3) TEU and reaffirmed on several occasions by the recent case-law of the Court of Justice.

LA PROMOZIONE DI STRUMENTI DI CO-REGOLAZIONE DELL'INTELLIGENZA ARTIFICIALE NELL'*AI ACT*, CON PARTICOLARE RIFERIMENTO ALLE *REGULATORY SANDBOXES*

Gabriele Rugani*

SOMMARIO: 1. Introduzione: la necessità di coinvolgere gli *stakeholders* nella regolamentazione dell'IA. – 2. Le *regulatory sandboxes*: definizione e analisi della prassi negli Stati UE. – 3. Le *regulatory sandboxes* nella proposta dell'*AI Act* della Commissione. – 4. Le *regulatory sandboxes* nelle posizioni del Consiglio e del Parlamento europeo. – 5. Le *regulatory sandboxes* nel testo finale dell'*AI Act*. – 6. Considerazioni conclusive: l'*AI Act* come strumento per promuovere una specifica modalità di disciplinare l'IA.

1. *Introduzione: la necessità di coinvolgere gli* stakeholders *nella regolamentazione dell'IA*

Nell'affrontare il tema della regolazione dell'intelligenza artificiale, ci si rende subito conto di quanto il coinvolgimento dei portatori di interessi si riveli sempre essenziale. Il dialogo con gli *stakeholders*, infatti, non ha esclusivamente la consueta finalità di aumentare la legittimazione democratica dei processi decisionali, interpellando tutti i soggetti interessati all'esito dei medesimi, ma ha soprattutto la funzione di aumentare l'*efficacia* dei suddetti processi: non si deve infatti dimenticare che si ha a che fare con una materia estremamente tecnica e complessa, in cui non si può prescindere dal decisivo apporto in termini di competenze ed esperienza degli specialisti del settore, quali soggetti pubblici, imprese, ONG e non solo[1].

Orbene, il regolamento (UE) 2024/1689 sull'intelligenza artificiale[2]

* Assegnista di ricerca post-dottorale in diritto dell'Unione europea e diritto pubblico comparato presso l'Università di Pisa (gabriele.rugani@jus.unipi.it). Prodotto realizzato all'interno del PRIN 2022 "*Artificial Intelligence between generating and tackling gender-based discriminations*" (AiGeDi), Unità dell'Università di Pisa.

[1] Sul punto v., *inter alios*, E. TRAMONTANA, *Organizzazioni non governative e ordinamento internazionale*, Padova, 2013.

[2] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

rappresenta una perfetta dimostrazione di come le istituzioni dell'Unione europea siano pienamente consapevoli delle suesposte esigenze di coinvolgimento degli interessati nella regolamentazione del settore. Ciò non solo per il fatto che l'*AI Act* è il frutto di un processo di consultazione degli *stakeholders* particolarmente lungo e articolato, svoltosi in seno all'UE a partire dal 2018 con la comunicazione della Commissione europea "L'intelligenza artificiale per l'Europa"[3], e intensificatosi nel 2020 con il "Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia" della Commissione medesima[4]; ma ancor di più per il fatto che tale regolamento promuove un successivo coinvolgimento dei portatori di interessi, incoraggiando l'utilizzo di ulteriori modalità, anche atipiche, di co-regolazione dell'IA.

Alla luce di quanto esposto, il presente contributo intende concentrarsi proprio su tali strumenti di co-regolazione della materia che l'*AI Act* tenta di incentivare, con particolare attenzione a quello rappresentato dalle c.d. "*regulatory sandboxes*", o "spazi di sperimentazione normativa"[5]. La tratta-

[3] Commissione europea, comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "L'intelligenza artificiale per l'Europa", COM (2018) 237final, 25 aprile 2018.

[4] Commissione europea, Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia, COM (2020) 65final, 19 febbraio 2020.

[5] Sulle *regulatory sandboxes* v., *inter alios*: L. Bromberg, A. Godwin, I. Ramsay, *Fintech sandboxes: achieving a balance between regulation and innovation*, in *Journal of banking and finance law and practice*, 2017, p. 314 ss.; G. Branellec, J. Lee, *Le choix du modèle de régulation des Fintech: entre* sandbox *et* soundbox, in *Revue d'économie financière*, 2019, p. 387 ss.; E. Corapi, *Regulatory Sandbox nel Fintech?*, in E. Corapi, R. Lener (a cura di), *I diversi settori del FinTech. Problemi e prospettive*, Milano, 2019, p. 13 ss.; M. T. Paracampo, *Dalle regulatory sandboxes al network dei facilitatori di innovazione tra decentramento sperimentale e condivisione europea*, in *Rivista di diritto bancario*, 2019, p. 219 ss.; M. Lesher, *Bringing new digitally enabled products and services to market: sandboxes and the role of policy experimentation*, in *cepr.org*, 2020; W. G. Ringe, C. Ruof, *Regulating Fintech in the EU: the Case for a Guided Sandbox*, in *European Journal of Risk Regulation*, 2020, p. 604 ss.; M. Gómez Santos, *Régimen jurídico del "regulatory sandbox" en España*, in *Revista de Derecho del Sistema Financiero: mercati, operadores e contratos*, 2021, p. 195 ss.; G. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti. Le regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normativa*, in *federalismi.it*, 2022, p. 88 ss.; A. Merlino, *Il regulatory sandbox. Una nuova prospettiva ordinamentale*, Napoli, 2022; A. Merlino, *Il regulatory sandbox e la teoria delle fonti*, in *Diritto pubblico europeo – Rassegna online*, 2022; M. T. Paracampo, *Il percorso evolutivo ed espansivo delle regulatory sandboxes da FinTech ai nuovi lidi operativi del prossimo futuro*, in *federalismi.it*, 2022, p. 207 ss.; M. Trapani, *L'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento*, in *Osservatorio sulle fonti*, 2022, p. 215 ss.

zione, preliminarmente, descriverà cosa si intende con tali espressioni; poi, ripercorrerà l'*iter legis* del regolamento, illustrando la disciplina che la Commissione aveva proposto per la materia, nonché i suggerimenti formulati dal Consiglio e dal Parlamento europeo; in seguito, analizzerà nel dettaglio la regolamentazione degli spazi di sperimentazione normativa a cui si è finalmente giunti nella versione ultima dell'*AI Act*; infine, sarà possibile svolgere alcune considerazioni di carattere conclusivo.

2. *Le* regulatory sandboxe*s: definizione e analisi della prassi negli Stati UE*

Stando alla definizione abbracciata a livello UE, segnatamente dal Consiglio, già da prima della proposta di regolamento sull'intelligenza artificiale, le "*regulatory sandboxes*" o "spazi di sperimentazione normativa" consistono in «quadri concreti che, fornendo un contesto strutturato per la sperimentazione, consentono, se del caso in un ambiente reale, di testare tecnologie, prodotti, servizi o approcci innovativi – al momento soprattutto nel contesto della digitalizzazione – per un periodo di tempo limitato e in una parte limitata di un settore o di un ambito soggetto a vigilanza regolamentare, garantendo la messa in atto di opportune misure di salvaguardia»[6]. Tale nozione va spesso e volentieri di pari passo con un altro concetto, quello di "*experimentation clauses*", o "clausole di sperimentazione": si tratta di «disposizioni giuridiche che consentono alle autorità incaricate di attuare e applicare la legislazione di esercitare, caso per caso, un certo grado di flessibilità in relazione alla sperimentazione di tecnologie, prodotti, servizi o approcci innovativi»; spesso e volentieri, esse costituiscono proprio la base giuridica degli spazi di sperimentazione normativa[7].

Detto in termini ancor più semplici, le *sandboxes* sono dunque spazi, virtuali oppure fisici, nei quali è possibile testare – per periodi limitati e sotto la sorveglianza di un'autorità competente – progetti innovativi sul piano tecnologico, con la possibilità di derogare alla normativa di settore, consentendo ai promotori di svolgere i *test* nella maniera più completa ed efficiente possibile, *test* a cui ovviamente partecipano i soggetti a vario titolo interes-

[6] Sul punto v. Consiglio dell'Unione europea, *Conclusioni del Consiglio sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale*, 16 novembre 2020, disponibile al seguente link: www.data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/it/pdf, p. 8.

[7] *Ibidem*, p. 9.

sati agli esiti. Esse sono caratterizzate da un'ulteriore peculiarità: i risultati della sperimentazione possono essere utilizzati come base per una successiva ed eventuale modifica normativa[8].

Nell'Unione europea, alcuni Stati membri hanno già fatto un certo ricorso a spazi di sperimentazione normativa. In Italia, ad esempio, tale strumento è stato introdotto, con il decreto-legge 30 aprile 2019 n. 34 detto "Decreto Crescita" (a cui è seguito il decreto 30 aprile 2021 n. 100 del Ministero dell'Economia e delle Finanze), nel settore della c.d. "finanza tecnologica" o "*fintech*" (ovvero quella parte del mondo finanziario in cui, sfruttando l'innovazione tecnologica, è possibile sviluppare nuovi modelli di *business*, processi, prodotti e anche nuovi operatori di mercato)[9]. Meritevole di menzione è anche l'iniziativa "Sperimentazione Italia", regolamentata dal decreto-legge 16 luglio 2020 n. 76 e segnatamente dal suo art. 36, caratterizzata dall'attenzione del legislatore alla c.d. "trasformazione digitale della pubblica amministrazione" e come tale avente natura multisettoriale[10]; essa ha trovato applicazione nell'ambito delle "*smart cities*" e ancor più precisamente nel settore della c.d. "*smart mobility*"[11].

Vi sono poi anche altri Stati membri UE che hanno fatto ricorso agli spazi di sperimentazione normativa. È infatti possibile citare la Spagna, che come l'Italia ha istituito una *sandbox* relativa al settore *fintech*; la Germania, che ha incentivato l'utilizzo di clausole di sperimentazione da parte dei singoli *Länder* in numerosi settori, tra cui ancora una volta quello del trasporto intelligente; il Portogallo, dove la sperimentazione si svolge in un luogo fi-

[8] M. Trapani, *op. cit.*, pp. 216-217.

[9] *Ibidem*, p. 229.

[10] *Ibidem*, p. 232.

[11] Su "*smart cities*" e "*smart mobility*", v. *inter alios*: M. Finck, M. Lamping, V. Moscon, H. Richter (eds.), *Smart Urban Mobility. Law, Regulation, and Policy*, Berlin, 2020. In particolare, sulla definizione di "*smart mobility*", v. *inter alios*: S. Ranchordás, *Smart Mobility, Transport Poverty and the Legal Framework of Inclusive Mobility*, in M. Finck, M. Lamping, V. Moscon, H. Richter (eds.), *op. cit.*, p. 61 ss., spec. p. 67, secondo cui: «Smart mobility is a novel and complex concept which refers to transportation and more broadly to mobility solutions based on IT. The concept of smart mobility has been defined in the literature by reference to four central elements: first, it includes vehicle technology (e.g. alternative fuels, electric mobility, autonomous driving and vehicle dynamics; second, it is supported by Intelligent Transport Systems such as connected vehicles or intelligent traffic management; third, it requires large amounts of data on transportation, weather and traffic conditions that corresponds to the real-time demand of passengers; fourth, it includes the development of new mobility services such as ride-sharing, new biking systems and multimodal transportation». Sul punto v. anche: H. Jeekel, *Social Sustainability and Smart Mobility: Exploring the relationship*, in *Transportation Research Procedia*, 2017, p. 4296 ss., spec. p. 4305.

sico definito "Zona Franca Tecnologica" (ZLT), ovverosia un'area geografica e "tematica" in cui sperimentare progetti tecnologicamente innovativi; e la Francia, che ha istituito *sandboxes* per il settore energetico, nonché per progetti relativi alla tutela e al trattamento dei dati personali in vari settori (come sanità e trasporti)[12].

In tutti questi casi, le *regulatory sandboxes* hanno consentito un'interazione e un dialogo tra i soggetti a vario titolo interessati, pubblici e privati, che all'interno degli "spazi" si sono fatti portatori delle proprie competenze e dei propri punti di vista, sempre al fine di superare le difficoltà tecniche o tecnologiche che si erano di volta in volta poste.

In definitiva, le *sandboxes* rappresentano un nuovo modello collaborativo di produzione normativa – particolarmente utile nel caso in cui la materia da disciplinare sia caratterizzata da un considerevole contenuto tecnologico – che comporta un superamento del tradizionale metodo di coinvolgimento degli *stakeholders* nel quale il legislatore, accogliendo i contributi di questi mediante procedure formalizzate e non, affronta l'attività di regolazione in modo generale ed astratto. La *sandbox* può infatti comportare una regolamentazione "dal caso concreto", estrapolando regole generali dal caso individuale che è frutto di un impulso dei portatori di interessi: un modello che presenta innumerevoli potenzialità[13].

3. *Le* regulatory sandboxes *nella proposta dell'*AI Act *della Commissione*

Dopo questo sintetico chiarimento terminologico, è possibile tornare all'*iter legis* del regolamento sull'intelligenza artificiale, e per prima cosa si descriverà la disciplina che la Commissione europea aveva delineato per le *regulatory sandboxes* all'interno della sua 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"[14].

Fin dai propri "Considerando", la proposta ricordava che l'IA «è una famiglia di tecnologie in rapida evoluzione che richiede nuove forme di sorveglianza regolamentare e uno spazio sicuro per la sperimentazione,

[12] M. TRAPANI, *op. cit.*, pp. 233-239.

[13] *Ibidem*, p. 228.

[14] Commissione europea, 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) 206final, 21 aprile 2021.

garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi»; perciò, si riteneva opportuno proprio «incoraggiare le autorità nazionali competenti […] a istituire spazi di sperimentazione normativa in materia di intelligenza artificiale», con l'obiettivo di «agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio»[15].

Conseguentemente la proposta, il cui intero Titolo V (artt. 53-55) riguardava le "Misure a sostegno dell'innovazione", dedicava l'art. 53 proprio agli "Spazi di sperimentazione normativa per l'IA". Tale disposizione prevedeva innanzitutto che siffatti spazi, istituiti dalle autorità competenti degli Stati membri oppure dal Garante europeo della protezione dei dati (GEPD), dovessero fornire un ambiente «che facilita lo sviluppo, le prove e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio»; ciò rigorosamente «sotto la guida e il controllo diretti delle autorità competenti» al fine di garantire il rispetto delle pertinenti normative tra cui, *in primis*, lo stesso regolamento sull'intelligenza artificiale (art. 53, par. 1).

Sul punto, era altresì stabilito che le autorità nazionali per la protezione dei dati personali, o le autorità che comunque forniscono o sostengono l'accesso ai dati, dovessero essere associate al funzionamento delle *regulatory sandboxes* qualora fossero coinvolti i loro ambiti di competenza (art. 53, par. 2) e che i poteri correttivi e di controllo delle autorità medesime non potessero essere pregiudicati dagli spazi di sperimentazione normativa (art. 53, par. 3).

Era poi previsto che i partecipanti alla *sandbox* dovessero rimanere responsabili ai sensi delle pertinenti regole per eventuali danni arrecati a terzi a seguito della sperimentazione (art. 53, par. 4); che le autorità competenti dovessero presentare alla Commissione europea relazioni annuali sull'attuazione degli spazi (art. 53, par. 5); nonché, infine, che le modalità e le condizioni di funzionamento delle *sandboxes*, tra cui i diritti e gli obblighi dei partecipanti, dovessero essere stabiliti in atti di esecuzione (art. 53, par. 6)[16].

[15] *Ibidem*, considerando n. 71.

[16] *Ibidem*, art. 53 ("Spazi di sperimentazione normativa per l'IA"), in base a cui: «1. Gli spazi di sperimentazione normativa per l'IA istituiti da una o più autorità competenti degli Stati membri o dal Garante europeo della protezione dei dati forniscono un ambiente controllato che facilita lo sviluppo, le prove e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico. Ciò avviene sotto la guida e il controllo diretti delle

4. *Le* regulatory sandboxes *nelle posizioni del Consiglio e del Parlamento europeo*

A questo punto, esaminata la disciplina proposta dalla Commissione in tema di *sandboxes*, è possibile soffermarsi sulle posizioni adottate in materia dal Consiglio e dal Parlamento europeo nel corso della procedura legislativa.

In generale, con riferimento all'approccio complessivamente tenuto dalle due istituzioni di cui sopra durante l'intero *iter legis* dell'*AI Act*, si potrebbe semplificare dicendo che, se il Consiglio è parso più attento a promuovere lo sviluppo dei sistemi di IA e a rendere il testo più vicino alle esigenze delle imprese, il Parlamento europeo è sembrato invece più sensibile alle istanze di protezione dei diritti dei cittadini e dei consumatori, circostanza che ha poi reso necessari rilevanti sforzi per negoziare un testo condiviso[17].

autorità competenti al fine di garantire la conformità ai requisiti del presente regolamento e, se del caso, di altre normative dell'Unione e degli Stati membri controllate all'interno dello spazio di sperimentazione. 2. Gli Stati membri garantiscono che, nella misura in cui i sistemi di IA innovativi comportano il trattamento di dati personali o rientrano altrimenti nell'ambito di competenza di altre autorità nazionali o autorità competenti che forniscono o sostengono l'accesso ai dati, le autorità nazionali per la protezione dei dati e tali altre autorità nazionali siano associate al funzionamento dello spazio di sperimentazione normativa per l'IA. 3. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi e di controllo delle autorità competenti. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi deve comportare l'adozione di immediate misure di attenuazione e, in mancanza di ciò, la sospensione del processo di sviluppo e di prova fino a che tali rischi non risultino attenuati. 4. I partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. 5. Le autorità competenti degli Stati membri che hanno istituito spazi di sperimentazione normativa per l'IA coordinano le loro attività e cooperano nel quadro del comitato europeo per l'intelligenza artificiale. Esse presentano al Comitato e alla Commissione relazioni annuali sui risultati dell'attuazione di tali sistemi, comprese le buone pratiche, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione del presente regolamento e di altre normative dell'Unione soggette a controllo nell'ambito dello spazio di sperimentazione. 6. Le modalità e le condizioni di funzionamento degli spazi di sperimentazione normativa per l'IA, compresi i criteri di ammissibilità e la procedura per la domanda, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione, nonché i diritti e gli obblighi dei partecipanti sono stabiliti in atti di esecuzione. Tali atti di esecuzione sono adottati in conformità alla procedura d'esame di cui all'articolo 74, paragrafo 2».

[17] Sul punto, mi sia concesso fare rinvio a: G. Rugani, *The European Parliament's Position on the AI Act: a human rights-oriented approach and an attempt to regulate generative AI systems*, in *BlogDUE*, 2023. V. anche, *inter alios*: C. Djeffal, *The EU AI Act at a crossroads:*

Per quanto riguarda più nello specifico gli spazi di sperimentazione normativa, tuttavia, entrambe le istituzioni si sono dimostrate d'accordo nel favorirli, andando addirittura oltre rispetto a quanto proposto dalla Commissione.

Infatti, nel suo "Orientamento generale" adottato in data 6 dicembre 2022, il Consiglio ha promosso l'idea secondo cui le *sandboxes* dovrebbero anche consentire di testare sistemi di IA innovativi «*in condizioni reali* [enfasi aggiunta]», sempre sotto il controllo delle autorità nazionali competenti (art. 53 dell'Orientamento generale); ha poi suggerito l'aggiunta di nuove disposizioni per permettere di testare sistemi di IA «in condizioni reali *al di fuori degli spazi di sperimentazione normativa* [enfasi aggiunta]», e dunque senza controlli, ancorché in presenza di condizioni e garanzie specifiche (art. 54 *bis* dell'Orientamento generale, dedicato proprio alle "Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA")[18].

Allo stesso modo, nella propria posizione negoziale del 14 giugno 2023, pure il Parlamento europeo ha posto particolare enfasi sulla necessità di incentivare le *regulatory sandboxes*. In particolare, nel suo testo ha inserito una disposizione di notevole rilievo secondo cui «[g]li Stati membri istituiscono *almeno uno* [enfasi aggiunta] spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in applicazione del presente regolamento» (art. 53, par. 1). Tra le altre cose, inoltre, il Parlamento ha promosso previsioni in base a cui «[p]ossono essere istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale o congiuntamente con altri Stati membri» (art. 53, par. 1, *bis*) e in base a cui «[a]nche la Commissione e il Garante europeo della protezione dei dati, da soli, congiuntamente o in collaborazione con uno o più Stati membri, possono istituire spazi di sperimentazione normativa per l'IA a livello dell'Unione» (art. 53, par. 1, *ter*)[19].

generative AI as a challenge for regulation, in *European Law Blog*, 24 July 2023.

[18] Sull'Orientamento generale del Consiglio, v. la pagina del sito ufficiale del Consiglio dal titolo "Normativa sull'intelligenza artificiale: il Consiglio chiede di promuovere un'IA sicura che rispetti i diritti fondamentali", pubblicata in data 6 dicembre 2022 e disponibile al seguente link: www.consilium.europa.eu/it/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/.

[19] Sulla posizione negoziale del Parlamento europeo, v. la pagina del sito ufficiale del Parlamento europeo dal titolo "Intelligenza artificiale: deputati pronti a negoziare le prime norme per un'IA sicura e trasparente", pubblicata in data 14 giugno 2023 e disponibile al seguente link: www.europarl.europa.eu/news/it/press-room/20230609IPR96212/deputati-pronti-a-negoziare-le-prime-norme-per-un-ia-sicura-e-trasparente.

5. *Le* regulatory sandboxes *nel testo finale dell'*AI Act

È ora possibile analizzare nel dettaglio la disciplina delle *regulatory sandboxes* a cui si è finalmente giunti nel testo finale del regolamento (UE) 2024/1689, frutto dell'accordo politico raggiunto tra i co-legislatori in data 9 dicembre 2023[20] e adottato il 13 giugno 2024.

Partendo, innanzitutto, dai considerando, il numero 138 ricorda come l'IA sia una famiglia di tecnologie in rapida evoluzione, che richiede sorveglianza regolamentare e uno spazio sicuro e controllato per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi. Per tali ragioni, «gli Stati membri dovrebbero garantire che le rispettive autorità nazionali competenti istituiscano *almeno uno* [enfasi aggiunta] spazio di sperimentazione normativa in materia di IA a livello nazionale», con l'obiettivo di «agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio».

Quanto alle disposizioni di interesse, esse sono contenute nel Capo VI (artt. 57-63), dedicato alle "Misure a sostegno dell'innovazione". Al suo interno, l'art. 57 riguarda proprio gli "Spazi di sperimentazione normativa per l'IA" e stabilisce che gli Stati membri «provvedono affinché le loro autorità competenti istituiscano *almeno uno* [enfasi aggiunta] spazio di sperimentazione normativa per l'IA a livello nazionale», che sia operativo entro il 2 agosto 2026 (art. 57, par. 1). In buona sostanza, nella versione definitiva dell'*AI Act* è stata recepita l'indicazione del Parlamento europeo, di cui si è detto sopra, nel senso di prevedere un vero e proprio obbligo per ciascun Paese UE di istituire almeno una *regulatory sandbox*.

È altresì previsto che possano essere istituite *sandboxes* aggiuntive «a livello regionale o locale, o congiuntamente con le autorità competenti di altri Stati membri» (art. 57, par. 2), oppure da parte del Garante europeo della protezione dei dati (art. 57, par. 3), anche in questo caso in linea con i suggerimenti del Parlamento.

Le *sandboxes* possono comprendere anche prove in «condizioni reali», comunque soggette a controllo nell'ambito dello spazio di sperimentazione (art. 57, par. 5); un aspetto che invece, lo si ricorderà, era stato promosso dal Consi-

[20] Sul punto, v. la pagina del sito ufficiale della Commissione europea dal titolo "Soddisfazione della Commissione per l'accordo politico sulla legge sull'intelligenza artificiale", pubblicata in data 9 dicembre 2023, e aggiornata in data 10 dicembre 2023, disponibile al seguente link: www.ec.europa.eu/commission/presscorner/detail/it/ip_23_6473.

glio.

L'art. 57 stabilisce poi che le autorità nazionali per la protezione dei dati e le autorità che forniscono o sostengono l'accesso ai dati devono essere associate al funzionamento della *regulatory sandbox* e partecipare al controllo nei limiti dei rispettivi compiti e poteri (art. 57, par. 10); che i poteri correttivi o di controllo delle autorità competenti non devono essere pregiudicati dagli spazi di sperimentazione normativa (art. 57, par. 11); e che i partecipanti alla *sandbox* restano responsabili secondo le pertinenti normative per eventuali danni arrecati a terzi a seguito della sperimentazione (art. 57, par. 12).

Le autorità nazionali competenti devono presentare, all'ufficio per l'IA istituito dalla Commissione ai sensi dell'art. 64, nonché al Comitato europeo per l'intelligenza artificiale di cui all'art. 65 (composto da un rappresentante per Stato membro), relazioni annuali «sui progressi e sui risultati dell'attuazione» degli spazi (art. 57, par. 16).

L'art. 58 del regolamento, inoltre, prevede che siano adottati da parte della Commissione degli atti di esecuzione che precisino le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione delle *sandboxes*. Tutto ciò, al fine di evitare un'eccessiva frammentazione nell'UE.

Infine, meritevole di menzione è anche l'art. 60, che consente prove di sistemi di IA «in condizioni reali *al di fuori degli spazi di sperimentazione normativa* [enfasi aggiunta]», e dunque senza i relativi controlli, purché in presenza di condizioni e garanzie specifiche. In particolare, è richiesto il rispetto di un «piano di prova in condizioni reali», ovverosia «un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali»[21]; spetta alla Commissione, per mezzo di atti di esecuzione, il compito di specificare nel dettaglio gli elementi del piano di prova (art. 60, par. 1). Inoltre, è richiesto che i soggetti delle prove in condizioni reali abbiano dato il proprio consenso informato *ex* art. 61 (rubricato proprio "Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA"): una garanzia ritenuta necessaria dal legislatore dell'UE proprio per il fatto che ci si trova al di fuori dell'ambiente controllato rappresentato dalla *regulatory sandbox*[22]. Giova ripetere che anche la possibilità delle prove in condizioni reali al di fuori degli spazi di sperimentazione normativa non era presente nella proposta della Commissione, ma è stata aggiunta su iniziativa del Consiglio.

[21] Regolamento (UE) 2024/1689, art. 3, n. 53).

[22] T. Buocz, S. Pfotenhauer, I. Eisenberger, *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, in *Law, Innovation and Technology*, 2023, p. 357 ss., spec. p. 385.

6. *Considerazioni conclusive: l'*AI Act *come strumento per promuovere una specifica modalità di disciplinare l'IA*

A seguito dell'indagine compiuta, è ora possibile svolgere alcune considerazioni conclusive. Il regolamento (UE) 2024/1689 sull'intelligenza artificiale, frutto di un processo di consultazione dei portatori di interessi assai lungo e articolato, svoltosi in seno all'UE a partire dal 2018 e ulteriormente intensificatosi nel 2020, è a sua volta molto attento a promuovere un successivo coinvolgimento degli *stakeholders*, incentivando l'utilizzo di ulteriori modalità, anche atipiche, di co-regolazione dell'IA.

Tra tali modalità, spiccano indubbiamente le *regulatory sandboxes*, i.e. spazi, virtuali oppure fisici, nei quali è possibile testare (per periodi limitati e sotto la sorveglianza di un'autorità competente) progetti innovativi sul piano tecnologico, con la possibilità di derogare alla normativa di settore, la quale potrà essere eventualmente modificata al termine della sperimentazione. Esse consentono quindi di svolgere *test* nella maniera più completa ed efficiente possibile, coinvolgendo tutti coloro che sono a vario titolo interessati agli esiti: soggetti pubblici, imprese, ONG e non solo, i quali, dialogando tra di loro, tentano di superare le difficoltà tecniche o tecnologiche che inevitabilmente si pongono in tema di IA. Un fenomeno che, negli ultimi anni, è già andato diffondendosi anche in Europa.

Orbene, l'*AI Act* tenta non solo di regolamentare, ma anche e soprattutto di favorire l'utilizzo degli spazi di sperimentazione normativa. Il Capo VI, e specialmente l'art. 57, disegna infatti una disciplina assai particolareggiata, prevedendo nello specifico che ciascuno Stato debba istituire a livello nazionale *almeno uno* spazio suddetto, ma offrendo anche un ulteriore ventaglio di opzioni e possibilità, tra cui persino quella di testare in condizioni reali, ma al di fuori delle *sandboxes* (nel rispetto di condizioni e garanzie). Le suddette sperimentazioni potranno portare, in futuro, anche a integrazioni e modifiche delle normative in materia di IA, sia a livello di Unione europea, ad esempio in sede di riesame del regolamento o di adozione di atti di esecuzione da parte della Commissione[23], sia a livello dei singoli Stati membri dell'UE.

In estrema sintesi, si potrebbe quindi affermare che con l'*AI Act* la Commissione, ma anche il Consiglio e il Parlamento (che hanno contribuito

[23] Sul punto v. in particolare l'art. 112 del regolamento sull'intelligenza artificiale, dedicato a "Valutazione e riesame".

a potenziare ulteriormente lo strumento delle *sandboxes*), non hanno voluto solo dettare una normativa dell'intelligenza artificiale, ma anche una vera e propria *modalità di disciplinare* tale ambito. Una modalità fondata sul continuo dialogo con gli interessati, i quali possono portare all'interno degli spazi di sperimentazione normativa le proprie competenze e i propri punti di vista, sempre al fine di superare le complesse e mutevoli sfide derivanti dall'incessante sviluppo dell'IA. Il tutto, giova puntualizzarlo, in piena coerenza con quanto previsto dai Trattati, nei quali, come noto, risiede il fondamento ultimo del coinvolgimento degli *stakeholders* nella regolazione: si pensi, in particolare, all'art. 10 TUE, secondo il cui par. 3: «Ogni cittadino ha il diritto di partecipare alla vita democratica dell'Unione. Le decisioni sono prese nella maniera il più possibile aperta e vicina ai cittadini»; ma ancor di più all'art. 11 TUE, secondo il quale occorre mantenere «un dialogo aperto, trasparente e regolare» (par. 2), nonché procedere «ad ampie consultazioni» (par. 3) delle parti interessate[24].

A questo punto, la sfida sarà ovviamente quella di verificare, da un lato, quanto il regolamento sarà effettivamente in grado di promuovere la diffusione degli strumenti illustrati e, dall'altro, se detti strumenti riusciranno a fare in modo che tutti i differenti punti di vista in materia siano effettivamente rappresentati.

[24] Sul punto v. E. Lironi, *Potential and Challenges of E-Participation in the European Union*, Bruxelles, Study for the European Parliament's Committee on Constitutional Affairs (AFCO Committee), 2016, p. 31 ss.

Abstract (ita)

Il presente contributo intende concentrarsi sul tentativo, da parte dell'*AI Act*, di promuovere strumenti finalizzati a coinvolgere i portatori di interessi nella co-regolazione dell'intelligenza artificiale, tra i quali spiccano le c.d. "*regulatory sandboxes*" o "spazi di sperimentazione normativa". Pertanto, preliminarmente, la trattazione descriverà cosa si intende con tali espressioni. Poi, ripercorrerà l'*iter legis* del regolamento, illustrando la disciplina che la Commissione europea aveva originariamente proposto per la materia, nonché i suggerimenti formulati dal Consiglio e dal Parlamento europeo. In seguito, analizzerà nel dettaglio le previsioni sugli spazi di sperimentazione normativa a cui si è finalmente giunti nella versione ultima del regolamento (UE) 2024/1689. Infine, svolgerà alcune considerazioni di carattere conclusivo sul rapporto tra l'*AI Act* e il tema della co-regolazione dell'intelligenza artificiale.

Abstract (eng)

The contribution focuses on the attempt by the AI Act to promote instruments aimed at involving stakeholders in co-regulation of artificial intelligence, among which stand out the so-called "*regulatory sandboxes*". Therefore, at first, the paper will explain the meaning of such notion. Then, it will retrace the legislative procedure of the regulation, describing the legal framework originally proposed by the European Commission and the suggestions formulated by the Council and by the European Parliament. Subsequently, it will analyse in details the provisions on regulatory sandboxes which were finally included in the ultimate version of regulation (EU) 2024/1689. At last, it will give some concluding remarks on the relationship between the AI Act and the issue of co-regulation of artificial intelligence.

IL DIRITTO D'AUTORE NELL'*AI ACT*: *ERROR* 404 – *PAGE NOT FOUND*?

Cristina Grieco*

SOMMARIO: 1. Introduzione. – 2. Obblighi connessi alla tutela del diritto d'autore previsti dall'*AI Act*. – 3. Il silenzio dell'*AI Act* sulla questione del riconoscimento della paternità delle opere generate da un algoritmo. – 4. Conclusioni.

1. *Introduzione*

Il diritto d'autore, tradizionalmente legato ai requisiti della creatività e dell'originalità, nel corso degli anni ha subito evoluzioni significative, confrontandosi con sfide e mutamenti culturali sempre più intensi. L'imporsi dell'intelligenza artificiale, particolarmente di quella generativa, sta costringendo i legislatori e i giudici a riconsiderare gli stessi fondamenti della materia, a partire dalla paternità umana dell'opera intellettuale.

L'esigenza di coniugare la tutela del diritto d'autore con l'innovazione tecnologica e i principi del libero scambio, anche di prodotti dell'intelletto, rappresenta una sfida fondamentale sul piano normativo, anche nel contesto europeo. Le implicazioni e, soprattutto, gli esiti di questa sfida, interessano tanto gli autori e i creatori, quanto, considerata la funzione utilitaristica del diritto d'autore, la società nel suo complesso[1].

* Ricercatrice in diritto dell'Unione europea, Università degli Studi di Macerata.

[1] U. IZZO, *Alle radici della diversità tra* copyright *e diritto d'autore, tecnologia, interessi e cambiamento giuridico*, Roma, 2010, p. 18 ss.; G. MORGESE, *La normativa internazionale ed europea sul diritto d'autore*, in *La Comunità internazionale*, n. 4, 2014, p. 569 ss.; E. BONADIO, N. LUCCHI, *How Far Can Copyright Be Stretched? Framing the Debate on Whether New and Different Forms of Creativity can be protected*, in *Intellectual Property Quarterly*, 2019, p. 115 ss., disponibile *online*; C. HEATH, A. KAMPERMAN SANDERS, A. MOERLAND (eds.), *Intellectual Property Law and the Fourth Industrial Revolution*, Alphen aan den Rijn, 2020; G. M. RUOTOLO, *Il Copyright UE tra libertà di informazione, diritti fondamentali e mercato unico digitale*, in *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, p. 37 ss.; ID., *Spirits in the Material World: Artificial Intelligence Act e responsabilità per la diffusione online di informazioni*, in *Sidiblog*, 26 October 2023, disponibile *online.*

I possibili rischi vanno valutati sotto una duplice prospettiva. Da una parte, potrebbe accadere che queste nuove tecnologie, se non adeguatamente governate, finiscano per intaccare e privare lo sforzo intellettuale puramente umano del valore economico che fino ad oggi gli è stato riconosciuto; dall'altra, la preoccupazione è che norme eccessivamente protettive nel settore della proprietà intellettuale, considerata l'enorme mole di dati di cui hanno bisogno gli algoritmi per essere addestrati, finiscano per scoraggiare gli investimenti, con un impatto diretto sul mercato interno e sulla competitività[2].

L'Unione europea recentemente è intervenuta a regolamentare il fenomeno intelligenza artificiale con una normativa[3] che al momento rappresenta un *unicum* nel panorama mondiale[4]. Le istituzioni, con questo atto, stanno provando a misurarsi con una realtà in continua e rapidissima evoluzione[5]. L'Europa, inoltre, nel nome dell'ormai noto "effetto

[2] Si veda M. Bonazzi, M. Rizzi, F. Duran, *Sfide dell'Intelligenza Artificiale: IA e Diritto d'autore*, in *Mondo internazionale*, 1° marzo 2024, disponibile *online*.

[3] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828. Si vedano per un commento generale al regolamento M. Castellaneta, *Intelligenza artificiale: arrivano i paletti europei*, in *ilSole24ore*, 13 luglio 2024, disponibile *online*; F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in questo *fascicolo speciale*. Con riferimento a specifici aspetti si vedano altresì, in questo *fascicolo speciale*, M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*; G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle regulatory sandboxes*; E. Cirone, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*; A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*; S. Villani, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*

[4] Mathieu Michel, sottosegretario di Stato belga per la Digitalizzazione, ha così commentato: «The adoption of the AI act is a significant milestone for the European Union. This landmark law, the first of its kind in the world, addresses a global technological challenge that also creates opportunities for our societies and economies. With the AI act, Europe emphasizes the importance of trust, transparency and accountability when dealing with new technologies while at the same time ensuring this fast-changing technology can flourish and boost European innovation», si veda la *press release* del Consiglio, *Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI*, 21 May 2024, disponibile *online*.

[5] L'obiettivo lo si evince chiaramente dal considerando n. 1 e dall'articolo 1, paragrafo

Bruxelles"[6] e aspirando a diventare un *hub* globale per le *policy* sul digitale, sta tentando di imporsi come *leader* normativo e tecnologico attraverso l'imposizione dei propri *standard* al mondo, sperando di replicare l'esperienza di successo del GDPR recepito in diversi ordinamenti. Peraltro, nel caso dell'*AI Act*, il successo atteso, quantomeno sulla carta, dovrebbe essere auspicabilmente ancora maggiore, grazie all'ampia clausola di applicazione territoriale prevista dal regolamento[7].

V'è però da dire che, dal punto di vista tecnologico, l'Europa sconta un ritardo importante rispetto ai blocchi statunitense e cinese, e non solo. Guardando al mercato e alle capitalizzazioni, le prime società che operano e investono nel settore dell'IA sono al momento americane, cinesi e israeliane[8]. Peraltro, dopo l'annuncio di Meta e Apple di sospendere,

1, dove si legge che «lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione».

[6] A. BRADFORD, *Effetto Bruxelles. Come l'Unione europea regola il mondo*, Torino, 2021.

[7] Si veda l'articolo 2 che delinea l'ambito di applicazione del regolamento in maniera molto ampia.

[8] Nvidia, società americana che produce *microchip*, è al momento la società più capitalizzata al mondo. Compaiono poi, tra le società maggiormente capitalizzate del settore, le ben note Microsoft, Apple, Alphabet, Amazon, Tesla, Meta, IBM, a seguire Palantir Technologies, Dynatrace Holdings, UiPath, SentinelOne e Mobileye Global, unica società israeliana. A levante le nuove *unicorn* si chiamano Zhipu AI, Moonshot AI, MiniMax e 01.ai, sono valutate tra i 1,2 miliardi e i 2,5 miliardi di dollari e puntano a emulare il successo delle rivali statunitensi. La Corte dei conti europea all'interno della relazione speciale, *Le ambizioni dell'UE in materia di intelligenza artificiale Per il futuro, una governance più forte e investimenti più consistenti e mirati sono essenziali*, 31 maggio 2024, disponibile *online*, ha evidenziato che «sebbene l'UE disponga di forti capacità di ricerca, queste non si traducono sufficientemente in risultati nell'economia e nell'industria europee. Nonostante la crescita globale del numero di brevetti nel settore dell'IA, nel 2021 meno del 4% delle domande di brevetto a livello mondiale provengono da Europa e Asia centrale, rispetto a circa il 17% per gli Stati Uniti e al 62% per l'Asia orientale e il Pacifico. Gli Stati Uniti sono da tempo in testa nella corsa all'IA e la Silicon Valley funge da polo globale per l'innovazione in materia di IA. I giganti tecnologici americani come Google, Microsoft e IBM sono in prima linea nella *R&I*; investono in *start-up* e cofinanziano programmi di ricerca pubblici. Il governo degli Stati Uniti ha inoltre riconosciuto l'importanza strategica dell'IA, avviando iniziative e finanziamenti

almeno per il momento, il lancio delle loro tecnologie di IA in Europa, vi è già chi ha osservato che in questo settore l'"effetto Bruxelles" potrebbe in realtà rivelarsi un *boomerang*. Il rischio, infatti, è che la nuova regolamentazione, invece di spingere altri Stati ad adottare *standard* omogenei e le multinazionali ad adeguare le proprie prassi commerciali per tenerne conto, finisca per scoraggiare gli investimenti, aumentando il divario tecnologico tra l'Europa e i due *competitor* tecnologicamente più avanzati[9].

Le problematiche evidenziate sono tutt'altro che semplici, anche in considerazione del fatto che dal 2021, anno in cui la Commissione europea ha presentato la proposta di regolamento, lo scenario è già profondamente mutato a causa della nascita e della diffusione esponenziale di sistemi di intelligenza artificiale generativa che hanno fatto seguito al lancio di ChatGPT ad opera di OpenAI[10]. Allo stesso modo, dall'entrata in vigore dell'*AI Act* alla sua completa applicazione[11], è molto probabile che tanto ancora cambierà in ambito tecnologico e la nuova normativa rischierà di risultare già obsoleta.

Tra le varie questioni, ha già assunto e sicuramente continuerà ad assumere rilievo quella inerente alla tutela del diritto d'autore, alla quale è dedicato in parte l'articolo 53 dell'*AI Act*[12].

mediante varie agenzie federali e tre programmi di ricerca inter-agenzie sull'IA (adottati nel 2016, 2019 e 2023) volti a mantenere la *leadership* del paese nel settore. Nel 2022, la spesa pubblica nell'IA ha raggiunto i 3,3 miliardi di dollari. Nel 2017, la Cina ha elaborato un piano di sviluppo dell'IA al fine di investirvi fondi pubblici e diventare il *leader* mondiale del settore entro il 2030. La Cina si affida anche a investimenti privati di giganti tecnologici quali Alibaba, Baidu e Tencent».

[9] S. Da Empoli, *Brussels effect al contrario. Tenere le IA di Apple e Meta fuori dall'Europa è controproducente*, in *HuffPost*, 23 giugno 2024, disponibile *online*.

[10] Il lancio è avvenuto nel 2022.

[11] Secondo l'articolo 113, l'*AI Act* entrerà in vigore venti giorni dopo la pubblicazione nella Gazzetta ufficiale UE e inizierà ad applicarsi a partire dal 2 agosto 2026, salvo per quanto riguarda: i divieti relativi a pratiche vietate (sei mesi dopo); i codici di buone pratiche (nove mesi dopo); le norme sui sistemi di IA per finalità generali, compresa la *governance* (dodici mesi dopo); gli obblighi per i sistemi ad alto rischio (trentasei mesi dopo). Nondimeno, per agevolare l'applicazione del regolamento la Commissione ha previsto l'*AI Pact*, ovvero un sistema che incoraggia i fornitori e i distributori di sistemi di IA a prepararsi per tempo e a intraprendere azioni per conformarsi ai requisiti e agli obblighi stabiliti dall'*AI Act* su base volontaria.

[12] «Articolo 53 Obblighi dei fornitori di modelli di IA per finalità generali – 1. I fornitori di modelli di IA per finalità generali: a) redigono e mantengono aggiornata la documentazione tecnica del modello, compresi il processo di addestramento e prova e i risultati della sua valutazione, che contiene almeno le informazioni di cui all'allegato XI

In particolare, per ciò che riguarda il rapporto tra diritto d'autore e intelligenza artificiale, sono essenzialmente due le problematiche che stanno emergendo: da una parte, si stanno moltiplicando le azioni legali volte a sostenere la lesione dei diritti d'autore dei titolari nei *dataset* utilizzati in maniera indiscriminata dalle aziende nelle fasi di addestramento degli algoritmi; dall'altra, stanno aumentando le richieste di riconoscere direttamente in capo ai sistemi di intelligenza artificiale la paternità di opere intellettuali realizzate senza – o quasi – intervento umano.

Il presente contributo intende dunque esaminare l'articolo 53 del regolamento per comprendere quali risposte offre – o tralascia di offrire – l'*AI Act* a queste problematiche e la loro adeguatezza con riferimento all'attuale scenario e a quello che si sta delineando per il prossimo futuro[13].

affinché possa essere trasmessa, su richiesta, all'ufficio per l'IA e alle autorità nazionali competenti; b) elaborano, mantengono aggiornate e mettono a disposizione informazioni e documentazione per i fornitori di sistemi di IA che intendono integrare il modello di IA per finalità generali nei loro sistemi di IA. Fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale, le informazioni e la documentazione: i) consentono ai fornitori di sistemi di IA di avere una buona comprensione delle capacità e dei limiti del modello di IA per finalità generali e di adempiere ai loro obblighi a norma del presente regolamento; nonché ii) contengono almeno gli elementi di cui all'allegato XII; c) attuano una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) n. 2019/790; d) redigono e mettono a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali, secondo un modello fornito dall'ufficio per l'IA. 2. Gli obblighi di cui al paragrafo 1, lettere a) e b), non si applicano ai fornitori di modelli di IA rilasciati con licenza libera e open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici. Tale eccezione non si applica ai modelli di IA per finalità generali con rischi sistemici. [*Omissis*]».

[13] Si vedano in prospettiva internazionalistica per un'analisi dei problemi più risalenti a quelli più recenti le riflessioni di R. Mastroianni, *Diritto internazionale e diritto d'autore*, Milano, 1997, pp. 368-370; G. Contaldi, *La tutela delle invenzioni nel sistema OMC. Esclusiva brevettuale e valori emergenti nella comunità internazionale*, Milano, 2009, pp. 58, 79 e 120 ss.; G. M. Ruotolo, *(Not) The End of Human Race: la Dichiarazione di Bletchley avvia la cooperazione internazionale in materia di intelligenza artificiale*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazio-*

2. *Obblighi connessi alla tutela del diritto d'autore previsti dall'AI Act*

Il problema della tutela del diritto d'autore, soprattutto con riferimento ai sistemi di intelligenza artificiale generativa, si pone in maniera significativa sia perché queste tecnologie per poter essere addestrate necessitano di grandi *dataset*, sia perché in prospettiva giuridica il diritto d'autore è generalmente considerato un diritto fondamentale[14]. Pertanto, il bilanciamento che deve essere effettuato tra la promozione della competitività e la tutela dei diritti dei titolari richiede particolare cautela.

Occorre evidenziare che si devono al Parlamento europeo gli emendamenti volti ad includere all'interno del regolamento norme intese a disciplinare, anche dal punto di vista della tutela della proprietà intellettuale, i modelli di IA per finalità generali. Nella proposta iniziale della Commissione, infatti, non si prevedeva una normativa quanto a questi sistemi – e non avrebbe potuto essere altrimenti – posto che, come ricordato, i primi sono stati lanciati solo nel 2022.

A titolo di disciplina generale, si prevede che i sistemi in parola, qualora non comportino rischi sistemici, siano chiamati a soddisfare alcuni requisiti limitati, ad esempio in materia di trasparenza, mentre quelli che determinano rischi sistemici dovranno rispettare regole più rigorose[15].

La questione dell'uso di materiale protetto dal diritto d'autore per l'addestramento dei modelli per finalità generali si sta ponendo in maniera sempre più pressante tanto che ha già dato origine a diverse dispute legali[16]. Da una parte si trovano gli autori, i creatori e gli artisti che temono di

nali, universali e regionali, sui temi di interesse della politica estera italiana, disponibile *online*.

[14] Per un'analisi del diritto d'autore in questa prospettiva si vedano, tra gli altri, M. Vivant, *Le droit d'auteur, un droit de l'homme?*, in *Revue Internationale du Droit d'Auteur*, 1997, p. 61 ss.; F. Dessemontet, *Copyright and Human Rights*, in J. C. Kabel, J. H. M. Gerard (eds.), *Intellectual Property And Information Law: Essays In Honour Of Herman Cohen Jehoram*, The Hague, 1998, p. 113 ss.; R. Mastroianni, *La tutela internazionale e comunitaria del diritto d'autore come diritto fondamentale dell'uomo*, in A. M. Gambino, V. Falce (a cura di), *Scenari e prospettive del diritto d'autore*, Roma, 2009, p. 13 ss.

[15] Si vedano in particolare i considerando nn. 85, 97, 99, 100, 101, 104, 106-115 e gli articoli 1, paragrafo 2, lettera e); 2, paragrafo 1, lettera a); 3 e capo V, articolo 51 ss.

[16] Tra gli studi legali più in vista che si occupano della materia vi è Joseph Saveri Law Firm, LLP, che sta patrocinando cause intentate da programmatori software *v.* Gi-

vedere il proprio lavoro utilizzato senza alcun tipo di remunerazione, ma anche di vedersi pian piano sostituire dalle macchine; dall'altra, ci sono le grandi multinazionali, come Apple e Microsoft, che sostengono che, senza l'utilizzo di materiale protetto, sarebbe impossibile addestrare gli algoritmi ed evocano la similitudine tra il processo di apprendimento di un bambino e quello dei sistemi artificiali[17]. In particolare, le *Tech Giants* avvertono che questa tipologia di cause potrebbe creare enormi ostacoli per la nascente industria europea dell'IA, mentre gli istanti sostengono che le aziende sono in debito per aver utilizzato il loro lavoro senza autorizzazione e senza adeguato compenso. A motivo di ciò, si stanno moltiplicando le cause aventi ad oggetto l'origine presuntamente illecita dei dati di *input* utilizzati per addestrare gli algoritmi, o cause nell'ambito delle quali si denuncia l'utilizzo fraudolento di immagini asseritamente protette, la cui paternità sarebbe però da attribuire a sistemi di intelligenza artificiale. Nel Regno Unito, la società Getty Images ha avviato una causa dinanzi alla High Court of Justice di Londra contro Stability AI, l'impresa proprietaria della piattaforma generativa di immagini Stable Diffusion. Secondo quanto si legge nel comunicato stampa, quest'ultima avrebbe violato i diritti di proprietà intellettuale, compreso il *copyright* sui contenuti di proprietà o rappresentati da Getty Images, copiando illegalmente ed elaborando milioni di immagini protette a fini di sfruttamento commerciale senza consenso. Si pensi anche all'eclatante caso del New York Times che nell'agosto 2023 ha bloccato il *web crawler* di OpenAI, vietando di fatto

tHub, OpenAI. L'accusa che muovono i programmatori a sistemi come Copilot, che lavorano soppiantando la scrittura manuale di parti di codice non particolarmente creativo o magari completano automaticamente operazioni di programmazione più routinarie con compilazioni automatizzate, è di aver copiato parti di codice da loro sviluppate. Nel caso *Sarah Silverman, Christopher Golden e Richard Kadrey v. OpenAI*, secondo le allegazioni attoree, OpenAI avrebbe allenato ChatGPT su enormi *database* contenenti libri per un totale di titoli superiore a quello ottenibile lecitamente tramite *scraping web*. I *software* così addestrati restituirebbero riassunti precisi dei libri senza alcun riconoscimento dei diritti d'autore. Ancora, nel caso *Sarah Andersen, Kelly McKernan, and Karla Ortiz v. Stability AI, Midjourney, and DeviantArt*, i sistemi visivi di intelligenza artificiale generativa di questi fornitori sarebbero capaci di produrre opere "nello stile di" vari artisti viventi, ledendone i diritti d'autore.

[17] «Just as a child learns language (words, grammar, syntax, sentence structure) by hearing everyday speech, bedtime stories, songs on the radio, and so on, a model "learns" language by being exposed — through training — to massive amounts of text» hanno sostenuto gli avvocati di Meta, si veda B. BRITTAIN, *How copyright law could threaten the AI industry in 2024*, in *Reuters*, 2 January 2024, disponibile *online*.

al *software* che analizza i contenuti della rete di usare i propri articoli per addestrare il programma di intelligenza artificiale. L'addebito è sempre il medesimo: ai sistemi di intelligenza artificiale sarebbero stati fatti ingurgitare dati da *training dataset*, in cui erano presenti opere protette, poi utilizzati per la produzione di *output* più efficienti «without consent, without credit, and without compensation» per gli autori e i detentori dei diritti di proprietà intellettuale. Anche attori, cantanti, doppiatori si sono dichiarati preoccupati del fatto che il diffondersi di sistemi di intelligenza artificiale, in assenza di adeguate barriere normative, possa portare alla lesione dei loro diritti di immagine. Negli Stati Uniti è già stata promossa una *class action* contro Stability AI e Midjourney AI, che avrebbero creato contenuti che violano i diritti di immagine.

Occorre dunque capire come l'*AI Act* affronti questo primo problema.

V'è da dire che per ciò che riguarda il rapporto tra diritto d'autore e nuove tecnologie, l'*AI Act* non include norme di dettaglio. Nondimeno, già a partire dal preambolo del regolamento, vi è un frequente riferimento e un monito al rispetto dei diritti di proprietà intellettuale, delle informazioni commerciali riservate e dei segreti aziendali[18].

Si impone, in particolare, il rispetto della direttiva (UE) n. 790/2019 (di seguito direttiva *copyright*)[19], specie per quanto attiene agli aspetti le-

[18] Si ricordano, in particolare, i considerando nn. 48, 88, 167, l'articolo 25, paragrafo 5, articolo 52, paragrafo 6, articolo 53, paragrafo 1, lettera b), articolo 78, paragrafo 1, lettera a); allegato VII, paragrafo 4.5.

[19] Direttiva (UE) n. 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive n. 96/9/CE e n. 2001/29/CE. Nell'impianto dell'art. 4 della direttiva *copyright*, l'autorizzazione da parte dei titolari dei diritti si reputa fornita *ex lege* in assenza di un loro esplicito diniego o "riserva", c.d. *opt-out*, e sempre che si tratti di materiali ai quali i terzi hanno "legalmente accesso". Da notare che di recente, all'esito della consultazione pubblica *Artificial Intelligence and Intellectual Property: copyright and patents: Government response to consultation*, il Governo del Regno Unito ha annunciato che procederà nella direzione dell'eliminazione di qualunque restrizione all'eccezione di *text and data mining*. Si vedano i commenti di S. Orlando, *Il diritto di Text and Data Mining (TDM) non esiste*, in *Rivista italiana di informatica e diritto*, n. 1, 2023, disponibile *online*; A. Papa, *La tutela del pluralismo informativo in rete*, in A. Papa (a cura di), *Il diritto d'autore nell'era digitale*, Torino, 2019, p. 31 ss.; C. Geiger, G. Frosio, O. Bulayenko, *Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU (October 17, 2019)*, in C. Saiz García, R. Evangelio Llorca (dirs.), *Propiedad intelectual y mercado único digital europeo*, Valencia, 2019, pp. 27-71; C. Geiger, *The Missing Goal-Scorers in the Artificial Intelligence Team: Of Big Data, the Fundamental Right to Research and the failed Text and Data Mining Limitations in the CSDM Directive*, in *Research Paper Series*, 2021, n.

gati allo *scraping*[20] delle banche dati, operazione necessaria per l'addestramento dei sistemi di intelligenza artificiale[21], e per il *text and data mining*[22]. Normalmente, per scopi scientifici, l'attività di *text and data mining,* a condizione che l'accesso sia avvenuto legittimamente, è permessa dalla direttiva *copyright* anche in assenza di autorizzazione, mentre l'attività di estrazione e riproduzione a scopo commerciale può avvenire solo quando l'utilizzo per tali fini non sia stato riservato in modo espresso dai titolari (c.d. *opt-out*).

Il considerando n. 105 dell'*AI Act* conferma questa impostazione. Ne consegue che l'estrazione e la riproduzione di dati non è consentita se tale utilizzo sia stato espressamente escluso dal titolare del diritto d'autore attraverso la facoltà di riserva riconosciuta dall'articolo 4 della direttiva *copyright*. In questi casi, dunque, gli sviluppatori di modelli di IA dovranno ottenere una specifica autorizzazione anche per le operazioni di *text and data mining*.

Inoltre, al fine di promuovere una concorrenza equa e condizioni di

66, pp. 383-394; European Commission, Directorate-General for Communication, *Study on copyright and new technologies: copyright data management and artificial intelligence, Publications Office of the European Union*, 2022, disponibile *online*. Si veda altresì l'interpretazione fornita dalla Corte di giustizia 29 luglio 2019, C-476/17, *Pelham*, nel quale la Corte ha negato che ricorresse una riproduzione nel caso in cui un musicista, esercitando la propria libertà delle arti, aveva prelevato un campione sonoro da un fonogramma altrui al fine di integrarlo, in forma modificata e non riconoscibile all'ascolto umano, in un nuovo fonogramma.

[20] Il *web scraping* è una particolare tecnica di *crawling*. Un *crawler* – chiamato anche *bot* o *spider* – è un software che ha lo scopo di raccogliere tutte le informazioni necessarie per indicizzare in modo automatico le pagine di un sito, analizzare i collegamenti ipertestuali e trovare associazioni tra termini di ricerca e classificarli. È largamente usato da tutti i motori di ricerca, a cominciare da Google, per offrire agli utenti risultati sempre aggiornati. Il *web scraping* serve a estrarre dati dalle pagine web per poi raccoglierli in database o tabelle locali per analizzarli. Si tratta di un sistema in grado di estrapolare una grande varietà di informazioni: dati di contatto, indirizzi di posta elettronica, numeri di telefono, così come singoli termini di ricerca o URL.

[21] Si vedano, in particolare, i considerando nn. 104, 105 e 106 e l'articolo 53 del regolamento – che, come ricordato *supra* disciplina gli obblighi dei fornitori di modelli di IA per finalità generali – che richiamano al rispetto dell'eventuale riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva *copyright*.

[22] Per *text e data mining* si intende il processo di trasformazione di testo non strutturato in un formato strutturato per identificare modelli significativi ed estrarre dati. Applicando avanzate tecniche analitiche e altri algoritmi di *deep learning*, le aziende sono in grado di esplorare e rilevare relazioni nascoste all'interno dei propri dati non strutturati.

parità tra operatori economici europei ed extraeuropei, all'interno del considerando n. 106 si evidenzia che i fornitori di modelli di IA per finalità generali dovrebbero mettere in atto prassi commerciali e politiche aziendali conformi alle norme europee in materia di diritto d'autore, che consentano di rispettare la riserva dei diritti espressa dai titolari a norma dell'articolo 4, paragrafo 3, della ricordata direttiva *copyright*. Tale obbligo, per evitare che si possa ottenere un vantaggio competitivo nel mercato dell'Unione applicando norme in materia di diritto d'autore meno rigorose, è esteso a qualsiasi fornitore che immetta sul mercato europeo un modello di IA per finalità generali, indipendentemente dalla giurisdizione e dalla normativa in tema di proprietà intellettuale operante nel luogo in cui siano state eseguite le operazioni di addestramento degli algoritmi.

Alcune cautele sono previste anche per i sistemi forniti in *open source*. Normalmente per quest'ultimi, qualora non presentino rischi sistemici e i parametri – compresi i pesi, le informazioni sull'architettura e sull'uso del modello – siano già stati resi pubblici, si prevede un esonero generalizzato dagli obblighi di trasparenza previsti normalmente per i fornitori di modelli generali. Tuttavia, per quanto riguarda specificamente il diritto d'autore, il considerando n. 104 evidenzia che in ogni caso debba essere esplicitato come sia stata garantita la conformità nel caso di utilizzo di dati protetti. Ciò in quanto, il rilascio di sistemi di IA per finalità generali con licenza libera e *open source* non necessariamente rivela informazioni sostanziali sui *dataset* utilizzati per l'addestramento degli algoritmi. Si prevede altresì che l'eccezione operante per i modelli di IA per finalità generali, concernente il rispetto dei requisiti relativi alla trasparenza, prescinda dagli obblighi di produrre una sintesi del contenuto utilizzato per il *training* dei sistemi e dall'attuare una politica volta a conformarsi alla normativa europea in tema di diritto d'autore[23].

A ciò si aggiunga che, al fine di aumentare la trasparenza circa la natura dei dati utilizzati nelle fasi di pre-addestramento e poi di addestramento dei modelli di IA per finalità generali, compresi testo e dati protetti, il considerando n. 107 chiarisce l'opportunità che i fornitori elaborino e mettano a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati. In particolare, le imprese sono chiamate a redigere e aggiornare la documentazione tecnica concernente i modelli – incluso il processo di addestramento e di prova, oltre ai risultati della valutazione – così come tutte le informazioni necessarie per lo sviluppo e l'integra-

[23] Considerando n. 104 e articolo 53, paragrafo 2.

zione del modello medesimo. In questo caso, tuttavia, l'obbligo in parola impone di tenere in considerazione un ulteriore parametro, ovvero l'esigenza delle imprese di proteggere i segreti commerciali e le informazioni aziendali riservate. A motivo di ciò, si prevede che ci si possa limitare ad una sintesi di respiro ampio e generale, anziché dettagliata sotto il profilo tecnico, che includa le principali raccolte o serie di dati che sono state inserite nell'addestramento del modello e che venga fornita una descrizione delle altre fonti di dati utilizzate. Il considerando evidenzia poi l'opportunità che a fornire un modello per la sintesi sufficientemente semplice ed efficace sia proprio l'Ufficio europeo per l'intelligenza artificiale[24], che è altresì investito del compito di controllare se il fornitore abbia o meno adempiuto a tali obblighi, senza però procedere a una valutazione di dettaglio dei dati di addestramento in termini di conformità alla normativa sul diritto d'autore.

Posto che il tessuto produttivo ed industriale europeo è strutturalmente molto lontano da quello americano e cinese, caratterizzato da grandi multinazionali, per tentare di non gravare in maniera eccessiva sulle piccole aziende e sulle *start-up*, che non dovrebbero essere costrette a sostenere costi eccessivi né essere scoraggiate rispetto all'uso di tali modelli, si prevede che tutti gli adempimenti imposti siano proporzionati e commisurati alle effettive dimensioni del fornitore. A motivo di ciò, non è richiesta l'osservanza di tali obblighi – seppure se ne auspichi il rispetto volontario[25] – per quanti sviluppano o utilizzano modelli per finalità non professionali o di ricerca scientifica. Nondimeno, tale limitazione non opera in relazione alla normativa in tema di diritto d'autore, con riferimento alla quale si prescinde dalle dimensioni o dalla tipologia di fornitore e, pertanto, tutti sono chiamati a rispettarla.

Occorre dunque ora capire come siano state tradotte in norme le indicazioni fornite dai considerando. Come si ricordava in apertura del presente scritto, la disposizione di riferimento in tema di diritto d'autore all'interno del regolamento è l'articolo 53 che, al paragrafo 1, lettera c)[26], impone l'ob-

[24] Decisione della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale (C/2024/1459). Curioso notare che la decisione della Commissione di istituire l'ufficio europeo sull'intelligenza artificiale sia stata presa sulla base dell'*AI Act*, quando non era ancora in vigore.

[25] Considerando n. 109.

[26] «1. I fornitori di modelli di IA per finalità generali: c) attuano una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790».

bligo per i fornitori di modelli di IA per finalità generali di attuare una politica volta a conformarsi al diritto europeo in materia di diritto d'autore e dei diritti ad esso collegati e, in particolare, ad individuare e rispettare, anche attraverso tecnologie all'avanguardia, un'eventuale riserva di diritti espressa a norma dell'articolo 4, paragrafo 3[27], della ricordata direttiva *copyright*.

A tutela degli autori è stato introdotto un obbligo di *clearance* preventivo che impone alle aziende, in ossequio ad un principio di trasparenza, di rendere noto l'eventuale utilizzo per le operazioni di *training* degli algoritmi di *set* di dati protetti da *copyright*[28].

A ben vedere, dunque, con riferimento alla tutela del diritto d'autore, l'obiettivo dell'*AI Act* sembra essere quello di rinforzare la normativa preesistente e, in particolare, come si è evidenziato, la direttiva *copyright*, introducendo meccanismi di trasparenza e di *accountability*. Lo scopo pare voler essere quello di offrire la possibilità ai titolari di potersi opporre all'uso di contenuti proprietari a fini di addestramento degli algoritmi, ovvero di richiedere una remunerazione per l'uso delle informazioni ricavabili da essi. Appare però opportuno accennare al fatto che l'impianto della direttiva *copyright* è stato pensato con lo scopo di valorizzare il prodotto dell'ingegno dell'autore di fronte al suo sfruttamento – ormai massivo – realizzato attraverso le nuove tecnologie, in modo da portare al riconoscimento di un'equa remunerazione dei titolari dei diritti e dell'obbligo per i *providers* di ottenere una licenza preventiva per la pubblicazione di contenuti protetti. Questo modello effettivamente avrebbe potuto essere utilizzato anche nel caso dei sistemi di intelligenza artificiale, sebbene con tutte le difficoltà pratiche del caso, ma non è questa la scelta operata dal legislatore europeo nel regolamento. Quest'ultimo, infatti, ha preferito fare ricorso esplicitamente alle ricordate eccezioni previste dalla direttiva *copyright*, che però non erano state pensate per questi sistemi, tanto che non si rinviene alcun riferimento all'intelligenza artificiale nel testo. Del resto, anche da un punto di vista cronologico, la direttiva si colloca in un

[27] «[*omissis*] 3. L'eccezione o la limitazione di cui al paragrafo 1 si applica a condizione che l'utilizzo delle opere e di altri materiali di cui a tale paragrafo non sia stato espressamente riservato dai titolari dei diritti in modo appropriato, ad esempio attraverso strumenti che consentano lettura automatizzata in caso di contenuti resi pubblicamente disponibili online».

[28] Ai sensi dell'articolo 53, paragrafo 1, lettere c) e d). Inizialmente, peraltro, si discuteva di adottare una posizione più netta che prevedeva il divieto completo di utilizzo di materiale protetto da *copyright* per addestrare i modelli generativi.

momento precedente al lancio sul mercato dei sistemi di IA generativa. Ne consegue che l'applicazione delle eccezioni richiamate e del meccanismo dell'*opt out* genera un possibile cortocircuito, il quale minaccia di minare la protezione del diritto d'autore.

Inoltre, un altro potenziale rischio connesso potrebbe essere quello di rallentare lo sviluppo delle tecnologie di intelligenza artificiale all'interno dell'Unione europea e dare vita ad addestramenti incompleti degli algoritmi, a cui potrebbe ricollegarsi tutta una serie di ulteriori problematiche legata ai possibili effetti discriminatori nei confronti di determinati gruppi riconnessi all'utilizzo di *dataset* parziali o poco rappresentativi[29].

Nondimeno, nonostante lo sforzo profuso dal Parlamento europeo, gli obblighi imposti dall'articolo 53 risultano piuttosto generici e non appaiono sufficienti a definire uno strumento efficace di protezione dei diritti di proprietà intellettuale. Si omette infatti di specificare come le *policy* aziendali debbano essere formulate per potersi considerare conformi alla normativa in tema di diritto d'autore e, inoltre, non viene chiarito cosa debba essere compreso nelle sintesi dei dati protetti utilizzati ai fini di addestramento degli algoritmi e quale debba essere il livello di dettaglio. Vi sono poi oggettive difficoltà pratiche nell'identificazione dei titolari dei diritti d'autore: si pensi, ad esempio, al settore delle opere musicali e al fatto che non esiste un *database* universale delle opere protette. A ciò si aggiunga che i diritti di proprietà intellettuale sono anche geograficamente frammentati e non vi è generalmente un obbligo di registrazione dell'opera – a differenza di quanto avviene nell'attiguo settore della tutela brevettuale.

Da ultimo, l'*AI Act* omette di dare indicazioni sul tipo di licenza e sulla remunerazione per lo sfruttamento dei contenuti per l'addestramento degli algoritmi, lasciando quindi un ampio margine all'autonomia negoziale tra privati.

Sarà inevitabile che le lacune evidenziate aprano all'intervento delle legislazioni e delle corti nazionali, chiamate a fornire risposte concrete, originando una non auspicabile frammentarietà che non appare adeguata a gestire le sfide globali poste dalle nuove tecnologie[30].

[29] Per un esame dei possibili profili di criticità tra AI e diritti dei singoli v. C. GRIECO, *Intelligenza artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023.

[30] È stato riportato dal Financial Times, *AI And Media Companies Negotiate Landmark Deals Over News Content*, 17 June 2023, che sarebbero in corso negoziazioni tra OpenAI, Google, Microsoft e Adobe da una parte, ed editori come News Corp, Axel Springer, The New York Times e The Guardian dall'altra, per discutere di eventuali accordi di remunerazione

3. *Il silenzio dell'AI Act sulla questione del riconoscimento della paternità delle opere generate da un algoritmo*

Come si accennava in apertura del presente scritto, i due requisiti usualmente ritenuti fondamentali per poter considerare un'opera tutelabile sono quelli della creatività e dell'originalità. L'essenza del diritto d'autore muta proprio perché, nel tempo e nello spazio, si modifica il modo di intendere questi due concetti, anche a causa dell'imporsi sulla scena di nuove tecnologie[31].

Nel corso dei decenni, l'interpretazione del concetto di creatività si è evoluta fino a raggiungere un primo approdo sicuro che collega la creatività di un'opera alla quantità e alla qualità del contributo offerto dall'autore. Riconoscere o meno un'opera come creativa porta ad interrogarsi anche sulla sua originalità. La risposta a tale quesito traccia il confine tra ciò che può e deve essere riconosciuto come meritevole di tutela e ciò che invece, configurandosi come un lavoro creativamente banale o scontato, può considerarsi di dominio pubblico. Il singolo autore chiaramente beneficia dell'originalità della sua opera sul piano economico, ma anche la collettività ne trae vantaggio come incentivo per la cosiddetta creatività derivata[32].

Nondimeno, non trattandosi di una scienza esatta e non essendo spesso fornite definizioni giuridiche delle nozioni di autore, di creatività e di origi-

simili ad un abbonamento per l'utilizzo dei loro contenuti al fine di addestrare modelli come ChatGPT di OpenAI e Bard di Google. Si veda A. Appella, *Tutela del diritto d'autore nell' AI Act: le (molte) questioni irrisolte*, in *Agenda Digitale*, 27 luglio 2023, disponibile *online*.

[31] Si ricorderà, ad esempio, quanto accaduto con la fotografia nella seconda metà dell'Ottocento. Oggi non permangono più dubbi sul fatto che una riproduzione fotografica possa considerarsi un prodotto creativo, ma fino a quel momento non era mai accaduto che una creazione, nella quale buona parte del lavoro veniva svolto da una macchina, risultasse passibile di *copyright*. Fu con il noto caso *Burrow-Giles Lithographic Company v. Sarony*, 111 U.S. 53 (1884) deciso dalla Corte Suprema degli Stati Uniti, il 17 marzo 1884, che si pervenne a questo esito. La Corte, con riferimento alla famosissima immagine "Oscar Wilde No. 18", stabilì che la fotografia non può essere intesa come una mera riproduzione oggettiva della realtà. Infatti, l'immagine risulterà inevitabilmente differente a seconda delle scelte creative operate dal fotografo, rivelando così la sensibilità artistica di quest'ultimo.

[32] L'articolo 2.3 della Convenzione di Berna per la protezione delle opere letterarie ed artistiche, del 9 settembre 1886, che ha avuto successive revisioni, fornisce una protezione delle opere derivate, infatti si proteggono le traduzioni, gli adattamenti, le riduzioni musicali e altre trasformazioni di un'opera letteraria o artistica, equiparandole a delle opere originali e senza pregiudizio dei diritti dell'autore dell'opera originale. Anche il diritto italiano dedica

nalità[33], il confine rimane labile e molto viene lasciato all'interpretazione del giudice.

È proprio all'interno di questi spazi di "incertezza" che si compie il processo evolutivo del diritto d'autore, oggi particolarmente rapido e irruento proprio a causa dell'imporsi sulla scena dell'intelligenza artificiale generativa, potenzialmente dotata di capacità "creatrice"[34].

Peraltro, quando si parla di IA generativa, è necessario ripensare e rivalutare gli stessi contenuti dei requisiti della creatività e dell'originalità necessari, come detto, a rendere un'opera degna di essere tutelata. Ciò in quanto, è certamente vero che questi sistemi sono in grado di dare vita a qualcosa di nuovo e anche magari di innovativo rispettando canoni di perfezione inimmaginabili per un soggetto umano – d'altronde la perfezione non è di questo

spazio a questa tipologia di opere, la cui disciplina è data dall'articolo 4 della l. 633/1941 (legge sul Diritto d'autore) novellata dalla l. 3 maggio 2019, n. 37 e ancor più recentemente dal d. lgs. 177/2021 con cui è stata recepita la direttiva *copyright*. Sul punto, si vedano M. Bonazzi, M. Rizzi, F. Duran, *op. cit*. Nello specifico, sul caso dei manga giapponesi, si veda Y. Okuda, *Initial Ownership of Copyright in Cinematographic Work under Japanese Private International Law*, in A. Bonomi, P. Volken (eds.), *Yearbook of Private Internationl Law*, München, 2009, p. 377 ss.

[33] Per alcune riflessioni sul tema dell'originalità e della creatività si vedano, tra gli altri, F. Macmillan, *Il diritto d'autore nell'era digitale: verso il declino dell'originalità dell'opera*, in G. Resta (a cura di), *L'Armonia del Diritto: Contributi ad una riflessione su diritto e musica*, Roma, 2019, p. 119 ss.; S. Vaidhyanathan, *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*, New York, 2001, p. 254 ss.; S. Guizzardi, *Il requisito della originalità delle opere dell'ingegno come armonizzato dalla Corte di Giustizia*, in *AIDA – Annali Italiani del diritto d'autore, della cultura e dello spettacolo*, vol. 29, 2020, p. 3 ss. In un'interessante pronuncia sul tema, la Corte di cassazione italiana ha chiarito che: «(...) il carattere creativo e la novità dell'opera sono elementi costitutivi del diritto d'autore sull'opera dell'ingegno (...) sia sotto il profilo della compiutezza espressiva, sia sotto il profilo della novità (...)»; ed ancora che il concetto di creatività «(...) non coincide con quello di creazione, originalità e novità assoluta, riferendosi, per converso, alla personale e individuale espressione di un'oggettività appartenente alle categorie elencata nell'art. 1 della legge n. 633 del 1941, di modo che un'opera dell'ingegno riceva protezione a condizione che sia riscontrabile in essa un alto creativo, seppur minimo, suscettibile di manifestazione nel mondo esteriore, con la conseguenza che la creatività non può essere esclusa soltanto perché l'opera consiste in idee e nozioni semplici, ricomprese nel patrimonio intellettuale di persone aventi esperienza nella materia (...)», Cassazione Civile, sez. I, del 28 novembre 2011, n. 25173.

[34] E. Bonadio, N. Lucchi, *How Far Can Copyright Be Stretched? Framing the Debate on Whether New and Different Forms of Creativity can be protected*, in *Intellectual Property Quarterly*, n. 2, 2019, pp. 115-135; M. Capparelli, *Le nuove frontiere del diritto d'autore alla prova dell'Intelligenza Artificiale*, in U. Ruffolo (a cura di), *Intelligenza Artificiale, il diritto, i diritti, l'etica*, Milano, 2020, pp. 335-343.

mondo ma potrebbe esserlo del mondo artificiale – ma è altrettanto vero che lo fanno sulla base di *input* forniti a monte da esseri umani. Normalmente, quindi, un algoritmo non può considerarsi creativo di per sé, ma al più può essere programmato per essere creativo.

Dal punto di vista europeo, nel corso del tempo la Commissione ha lasciato liberi gli Stati membri di stabilire autonomamente gli *standard* medi di creatività e originalità richiesti ad un'opera per poter beneficiare della protezione autoriale. Per ciò che attiene alle opere generate attraverso l'intelligenza artificiale è stato predisposto un *test*[35], in base al quale le condizioni imprescindibili – ma non anche sufficienti – da vagliare per riconoscere una qualche forma di tutela sono eminentemente tre: deve trattarsi di una produzione in ambito letterario, scientifico o artistico; deve essere il risultato dello sforzo intellettuale umano; tale impegno deve riflettersi nell'*output*.

Questa impostazione si esprime molto chiaramente anche nella giurisprudenza europea che ha contribuito, in qualche modo, ad orientare l'interprete tentando di delineare i contenuti, particolarmente con riferimento a *software* e banche dati[36], due settori in cui la creatività e l'originalità sono caratteristiche più difficilmente individuabili e circoscrivibili. Nella pronuncia *Infopaq*[37], la Corte ha stabilito che un'opera dell'ingegno può dirsi originale se riflette la creazione intellettuale dell'autore. Il medesimo principio è stato enunciato nel caso *Painer*[38], laddove la Corte ha chiarito che l'opera può essere considerata originale se è possibile dimostrare l'attività dell'autore nel compiere delle scelte libere e creative nell'atto dell'ideazione. Ancora,

[35] Cfr. European Commission, Directorate-General for Communications Networks, Content and Technology, C. Hartmann, J. Allan, P. Hugenholtz et al., *Trends and developments in artificial intelligence – Challenges to the intellectual property rights framework – Final report, Publications Office of the European Union*, 2020, disponibile *online*.

[36] In base a quanto dispone la direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche dati, queste ultime beneficiano di una tutela *sui generis* poiché pur non essendo opere dell'ingegno, potrebbero comunque ricevere protezione in ragione degli ingenti investimenti finanziari di colui che ha provveduto alla sua costituzione. Si veda Corte giust. 1° marzo 2012, C-604/10, *Football Dataco Ltd* che in qualche modo ripropone quanto statuito precedentemente dalla Corte Suprema Americana, nella sentenza del 27 marzo 1991, *Feist Publications Inc./Rural Telephone Service Company Inc.*, con commento di A. Zoppini, in *Il Foro italiano*, vol. 115, 1992, pp. 37-44, in cui si afferma che il requisito dell'originalità sussiste se la banca dati è una creazione autonoma ed indipendente nella scelta ed organizzazione dei dati e se il risultato della predetta creazione non sia banale nella disposizione.

[37] Corte giust. 16 luglio 2009, C-5/08.

[38] Corte giust. 1° dicembre 2011, C-145/10, punto 2.5.

nel caso *Football Dataco Ltd*[39], la Corte ha stabilito, in via pregiudiziale, ed in conformità con la direttiva n. 96/9/CE, che: «(...) una banca dati ai sensi dell'articolo 1, paragrafo 2 (...) è protetta dal diritto d'autore (...) a condizione che la scelta o la disposizione dei dati in essa contenuti costituisca un'espressione originale della libertà creativa del suo autore (...)».

Da questa giurisprudenza emerge però, come in realtà i confini tra i requisiti dell'originalità e della creatività, quando si parla di proprietà intellettuale, finiscano per sfumare e confondersi, non potendo l'uno prescindere dall'altro.

La problematica connessa al riconoscimento della paternità ad opere realizzate da un sistema di intelligenza artificiale non si limita solo all'Europa, visto il moltiplicarsi delle richieste giunte all'esame di uffici amministrativi e, in alcuni casi, arrivati addirittura all'attenzione delle autorità giurisdizionali[40], sia nel settore della proprietà intellettuale sia in quello attiguo della tutela brevettuale.

In pratica, ci si interroga se sia o meno possibile poter riconoscere la paternità di testi, immagini, video, audio, codici e, in generale, di un'opera, all'algoritmo che li ha generati o se, al contrario, debba essere attribuita a chi fornisce le istruzioni dovendo ancora considerare una *condicio sine qua non* il *prompt*[41] umano[42], e quali risposte fornisce – od omette di fornire – l'*AI Act* sulla questione.

Occorre sin da subito evidenziare una lacuna nel regolamento su questo specifico punto. L'*AI Act*, infatti, rimane silente quanto al problema di

[39] *Football Dataco Ltd*, sopra citata.

[40] Ci si riferisce, in particolare, al noto caso Thaler, che ha richiesto di riconoscere la titolarità di un dipinto denominato A Recent Entrance to Paradise ad un sistema informatico brevettato, noto come Creativity Machine, di sua proprietà. Lo US Copyright Office ha opposto un primo diniego chiarendo che l'opera «lack[ed] the human authorship necessary to support a copyright claim», Copyright Office Refusal Letter, 12 August 2019 ("First Refusal Letter") at 1, ECF No. 13-4. Il ricorrente ha però richiesto all'ufficio di riconsiderare la propria domanda, contestando la necessità del requisito della paternità umana e sottolineando, ancora una volta, che l'opera era stata generata autonomamente dall'IA. Il Copyright Office ha opposto un nuovo diniego ribadendo che «[b]ecause copyright law is limited to "original intellectual conceptions of the author", the Office will refuse to register a claim if it determines that a human being did not create the work». Questioni simili sono emerse nei casi Portrait of Edmond de Belamy, The Next Rembrandt, The Day a Computer Wrote a Novel, AI-VA, Libro di Urantia, il Selfie scattato dal macaco Naruto e Théâtre D'opéra Spatial.

[41] Un *prompt* è un testo in linguaggio naturale che richiede all'IA generativa di eseguire una determinata attività.

[42] J. NAUGHTON, *Can AI-generated art be copyrighted? A US judge says not, but it's just a matter of time*, in *The Guardian*, 26 August 2023, disponibile *online*.

accordare tutela in forza del diritto d'autore alle opere generate da sistemi di intelligenza artificiale, lasciando così la questione aperta e, soprattutto, gravando i giudici del difficile compito di confrontarsi con le pressanti nuove istanze in materia, senza avere adeguati strumenti normativi a supporto.

La soluzione, dunque, andrà ricercata altrove. Un aiuto in tal senso arriva dalla risoluzione n. 2020/2015 del Parlamento europeo sui diritti di proprietà intellettuale e le tecnologie generate dall'intelligenza artificiale[43], che precisa che il concetto di creazione intellettuale non possa prescindere dalla personalità dell'autore umano e che dotare le tecnologie di intelligenza artificiale di personalità giuridica avrebbe ripercussioni negative sugli autori persone fisiche[44]. Pertanto, al fine di rispettare il principio di originalità, che è appunto ancora legato ad un soggetto umano, e dal momento che il concetto di "creazione intellettuale" riguarda la personalità dell'autore, il Parlamento nega la possibilità che le opere prodotte autonomamente da agenti artificiali e *robot* possano ritenersi ammissibili alla tutela ai sensi della normativa sul diritto d'autore.

Partendo da tale assunto, il Parlamento ha invitato la Commissione a sostenere un approccio orizzontale tecnologicamente neutrale basato su dati concreti in merito alle disposizioni comuni e uniformi in materia di diritti d'autore applicabili alle opere generate dall'IA nell'Unione, raccomandando, comunque, anche qualora si ritenesse tali opere ammissibili alla tutela ai sensi del diritto d'autore, che la titolarità di eventuali diritti sia assegnata soltanto alle persone fisiche o giuridiche che hanno creato l'opera in modo lecito e unicamente se il titolare dei diritti d'autore abbia concesso l'autorizzazione in caso di utilizzo di materiale protetto.

Tale approccio, tuttavia, non si riflette nel testo del regolamento che, come evidenziato, su questo punto rimane silente. Sotto un profilo strettamente giuridico, questa lacuna si configura come una grave mancanza da parte del legislatore europeo e apre a delle difficoltà che non potranno essere ignorate ancora a lungo. Quella della tipologia di riconoscimento e dei margini consentiti di estensione della tutela con riferimento all'*output* generato da un sistema di intelligenza artificiale, infatti, resta una questione centrale destinata ad assumere un rilievo ancora maggiore nel prossimo futuro, tenuto conto del moltiplicarsi di richieste in questo senso provenienti da più parti.

Il problema è che, allo stato attuale della normativa e della giurispru-

[43] Risoluzione del Parlamento europeo, del 20 ottobre 2020, sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale (2020/2015(INI)).

[44] *Ibidem*, punti 14 e 15.

denza[45], non pare possibile considerare un'opera generata utilizzando un sistema di intelligenza artificiale tutelabile, posto che difetterebbe della necessaria componente umana. Tuttavia, a ben vedere, applicando i canoni della creatività e originalità richiesti dall'attuale quadro normativo, nemmeno il programmatore potrebbe rivendicare la paternità dell'opera, dato che, nel caso dei sistemi di intelligenza artificiale generativa, mancherebbe – o risulterebbe del tutto marginale – il suo contributo. Il rischio è che queste opere restino prive di protezione, poiché il concetto di opera creata interamente da una macchina, anche se guidata e supervisionata dall'essere umano, rimane al di là dell'attuale portata giuridica e che, quindi, venga scoraggiato, anche da parte degli autori, l'utilizzo dei sistemi in questione, con conseguente freno all'innovazione.

L'*AI Act* avrebbe potuto essere un'ottima occasione per il legislatore europeo per affrontare questo problema, magari prevedendo nuove forme di licenze o di diritti d'autore "ibridi" che si adattino all'era dell'intelligenza artificiale. Esse potrebbero includere licenze specifiche dedicate ad opere generate dall'intelligenza artificiale o nuovi tipi di protezione che riflettano la natura collaborativa di molte opere create con l'ausilio dell'intelligenza artificiale[46].

4. *Conclusioni*

Le problematiche legate alla tutela del diritto d'autore e al rapporto con le nuove tecnologie di intelligenza artificiale sono ancora lontane dal trovare una soluzione definitiva, e, ciò nonostante, l'entrata in vigore di una delle normative al momento più avanzate e omnicomprensive in tema di intelligenza artificiale, come l'*AI Act*.

All'interno del testo vi è un generale richiamo al rispetto dei diritti dei titolari nei dati, eppure l'obbligo di *clearance* preventivo a carico delle azien-

[45] Bundespatentgericht 18 W (pat) 28/20, (Aktenzeichen) Verkündet am 21. Juni 2023. Diversamente, nel senso di un'apertura al riconoscimento della paternità alle opere generate da sistemi di intelligenza artificiale, Cassazione Civile, ordinanza n. 1107, del 9 gennaio 2023, pubblicata in data 16 gennaio 2023 e in maniera ancora più convinta Nanshan District People's Court, Shenzhen Tencent Computer System Co. Ltd. v. Shanghai Yingxun Technology Co. Ltd. ((2019) Yue 0305 Min Chu 14010) ((2019) 粤0305民初14010号), del 24 dicembre 2019).

[46] Si vedano le riflessioni di B. MARTINO, *Intelligenza artificiale e diritto d'autore, problematiche e casi di studio*, in *Legal for Digital*, 15 aprile 2024, disponibile *online*.

de e gli obblighi di trasparenza rischiano di risultare poco efficaci nella pratica e poco protettivi. La mole di dati utilizzata è talmente imponente che risulterà molto difficile controllare l'effettivo rispetto dei diritti dei titolari.

Su questo specifico punto v'è da dire che l'Europa si pone, anche normativamente parlando, più indietro rispetto a Cina e Stati Uniti.

Nel maggio del 2023, infatti, la Cyberspace Administration of China, ovvero la principale autorità deputata al controllo di Internet nel Paese, ha approvato una serie di linee guida per regolamentare il settore dell'AI generativa[47]. Il *focus* di queste regole è sulla promozione dell'innovazione nel campo dell'AI generativa e sul sostegno alle imprese e agli istituti che contribuiscono all'innovazione tecnologica. Nonostante ciò, i fornitori, conformemente al regolamento relativo alla gestione delle raccomandazioni sugli algoritmi dei servizi di informazione su Internet[48], sono chiamati a effettuare controlli di sicurezza e a registrare i loro algoritmi presso il governo, qualora i propri servizi siano in grado di influenzare l'opinione pubblica. Inoltre, le linee guida prevedono un obbligo di rispettare i diritti di proprietà intellettuale nei dati utilizzati nei processi di formazione di AI generativa, stabilendo espressamente che i fornitori e gli utenti dei servizi di AI generativa dovranno rispettare i diritti di proprietà intellettuale e l'etica commerciale, proteggere i segreti commerciali e non praticare il monopolio o la concorrenza sleale sfruttando algoritmi, dati, piattaforme e altri vantaggi[49].

Il legislatore cinese si è spinto oltre, prevedendo altresì che i fornitori di servizi, nello svolgimento delle attività di trattamento dei dati di addestramento, nel caso in cui siano coinvolti diritti di proprietà intellettuale, non dovranno in alcun modo violare tali diritti e i relativi interessi altrui.

Del resto, la prospettiva cinese in tema di tutela del diritto d'autore per le opere create attraverso l'uso di AI generativa si differenzia, come ricordato, dall'approccio strettamente antropocentrico adottato dall'Unione europea, anche grazie ad una definizione piuttosto ampia di "opera" che ha addirittura consentito all'autorità giurisdizionale cinese di mostrare un'apertura verso il riconoscimento della protezione anche ad opere ge-

[47] Interim Measures for the Administration of Generative Artificial Intelligence Services 生成式人工智能服務管理暫行辦法, 13 July 2023, disponibili *online* al seguente indirizzo www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.

[48] Provisions on the Administration of Internet Information Service Algorithm Recommendations 互联网信息服务算法推荐管理规定, 4 January 2022, disponibili *online* allo stesso indirizzo.

[49] Articolo 4, paragrafo 3; articolo 7, paragrafo 2.

nerate da sistemi di intelligenza artificiale al fine di promuovere l'innovazione[50].

Si può dunque evidenziare nelle scelte operate dal legislatore cinese uno sforzo maggiore di regolamentazione rispetto a quello profuso dalle istituzioni europee, posto che, in assenza di indicazioni più puntuali, non è effettivamente chiaro quale debba essere il perimetro dell'obbligo di *clearance* preventivo previsto nell'*AI Act* che pertanto rischia, come ricordato, di rivelarsi poco efficace e scarsamente protettivo rispetto al diritto dei titolari.

Quanto agli Stati Uniti, appare interessante l'approccio olistico promosso per affrontare il problema della tutela dei diritti di proprietà intellettuale, che evidenzia una diversa consapevolezza rispetto a quella mostrata dalle istituzioni europee rispetto al tema. L'amministrazione Biden, infatti, ha dichiarato di ritenere la "questione intelligenza artificiale" cruciale per lo sviluppo dell'economia americana[51] e per questo ha messo in moto una macchina considerevole. Lo US Copyright Office sta conducendo uno studio sui problemi di *copyright* sollevati dall'intelligenza artificiale generativa[52], con la finalità di raccogliere informazioni concrete e opinioni rilevanti per le politiche sul *copyright* così da consentire di valutare le potenziali aree di intervento da parte del Congresso. Quanto alla "questione *copyright*", con l'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, firmato dal Presidente Biden il 30 ottobre 2023[53], si impone una serie di obblighi in capo al Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO Director), tra cui la formulazione di raccomandazioni al Presidente su potenziali azioni esecutive relative al *copyright* e all'IA che dovranno affrontare tutte le questioni relative al diritto d'autore e i temi correlati, compresi la portata della protezione per le opere prodotte utilizzando l'IA e il trattamento delle opere protette da diritto d'autore nella formazione sull'IA. Inoltre, è previsto, per aiutare gli sviluppatori di algoritmi, l'incremento di un programma di formazione,

[50] P. Furiosi, G. Gialletti, *La Cina batte i record per la regolamentazione dell'Intelligenza artificiale: il primo regolamento sull'AI generativa in vigore dal prossimo 15 agosto*, in *NTplus Diritto*, 26 luglio 2023, disponibile *online*.

[51] Nella pagina del sito ww.//ai.gov/actions/, si legge «AI is a top priority for President Biden, and the Biden-Harris Administration is taking important steps to promote the safe, secure, and trustworthy use of AI».

[52] Tutte le informazioni sono reperibili all'interno del sito dello U.S. Copyright Office.

[53] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, firmato dal Presidente Biden, 30 October 2023, disponibile *online*.

analisi e valutazione per mitigare i rischi concernenti la proprietà intellettuale legati all'IA[54].

In conclusione, posto tutto quanto sopra esaminato, si può dire che, con riferimento al problema del diritto d'autore, l'*AI Act* rappresenta un'occasione mancata per il legislatore europeo che non ha fornito – ove ne ha fornita una peraltro – risposte particolarmente puntuali o esaustive. La questione quindi, alla luce di come la problematica si sta delineando nella pratica, rimane ancora più che mai aperta dal punto di vista sia della disciplina di dettaglio del diritto d'autore con riferimento ai sistemi di intelligenza artificiale, sia del possibile riconoscimento della paternità ad opere generate direttamente da sistemi di intelligenza senza, o quasi, intervento umano, e richiederà certamente nel prossimo futuro un nuovo intervento da parte della Commissione europea.

[54] Articolo 5.2, lettera c).

Abstract (ita)

L'avvento dell'intelligenza artificiale sta tra l'altro ridefinendo i canoni tradizionali del diritto d'autore. In particolar modo, due problematiche stanno emergendo: da una parte, si stanno moltiplicando le azioni legali volte a sostenere la lesione dei diritti d'autore dei titolari nei *dataset* utilizzati in maniera indiscriminata dalle aziende nelle fasi di addestramento degli algoritmi; dall'altra, stanno aumentando le richieste di riconoscere la paternità direttamente in capo ai sistemi di intelligenza artificiale di opere intellettuali realizzate senza – o quasi – intervento umano. Il contributo analizza tali temi a partire dalle soluzioni (per la verità, evanescenti) offerte dal nuovo regolamento dell'Unione europea sull'intelligenza artificiale.

Abstract (eng)

Among other things, the rise of artificial intelligence is redefining the traditional canons of copyright law. In particular, two issues are emerging: on the one hand, legal actions are multiplying to claim infringement of the copyrights of the owners of datasets used indiscriminately by companies in the algorithm training phases; on the other hand, requests to recognise the authorship directly to artificial intelligence systems of intellectual works realised without – or almost without – human intervention are increasing. This paper analyses those issues starting from the (to be honest, evanescent) solutions offered by the new EU Regulation on Artificial Intelligence.

PRIME RIFLESSIONI SULL'APPLICAZIONE DEL NUOVO REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE AL SETTORE SANITARIO

Sarah Lattanzi[*]

SOMMARIO: 1. Introduzione. – 2. I sistemi di IA impiegati in ambito sanitario e gli obblighi per i sistemi c.d. "ad alto rischio". – 3. Il problema della coerenza con altri strumenti legislativi. – 3.1. *Segue*: la coerenza con la legislazione verticale. – 3.2. *Segue*: la coerenza con il GDPR. – 3.3. *Segue*: la coerenza con il regolamento europeo sullo spazio europeo dei dati sanitari e con il regolamento relativo alla *governance* europea dei dati. – 3.4. *Segue*: la coerenza con la legislazione in via di adozione. – 4. Brevi riflessioni conclusive.

1. *Introduzione*

È verosimile che l'applicazione del nuovo regolamento sull'intelligenza artificiale[1] (IA) risulterà alquanto incisiva nei c.d. "settori ad alto impatto" tra cui figurano l'ambiente, la finanza e la sanità[2]. In quest'ultimo[3], numerose

[*] Ricercatrice in diritto dell'Unione europea presso l'Università degli Studi di Napoli Parthenope.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Per un commento si v. questo *fascicolo speciale* e C. SCHEPISI, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, p. 53 ss.; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, p. 415 ss.; O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *La proposta di Regolamento sull'intelligenza artificiale: Verso una nuova governance europea*, in *Agenda Digitale*, 2021.

[2] Si v. 1.1: «Motivi e obiettivi della proposta», in 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) 206final, 21 aprile 2021.

[3] Il settore sanitario è definibile come l'insieme di norme, istituti, servizi, attività e attori che contribuiscono alla creazione di un sistema di supporto destinato alla promozione, al

e promettenti appaiono le ipotesi applicative di sistemi e tecnologie basate sulla intelligenza artificiale[4].

Questi potranno essere usati in ambito sanitario per il miglioramento delle previsioni statistiche atte a valutare l'insorgenza e la diffusione di una pandemia; potranno coadiuvare il medico nella diagnosi e nella personalizzazione della cura; o ancora ottimizzare le operazioni di routine come l'assegnazione delle risorse nelle strutture ospedaliere[5]. Come è stato notato, in questo ambito i sistemi di intelligenza artificiale potranno essere sfruttati praticamente in tutte le fasi di assistenza, da quella della ricerca a quella dell'erogazione del servizio sanitario[6].

A seconda dei compiti che si intendono perseguire, diversi saranno i modelli di IA da sfruttare[7]: applicazioni di aumento della realtà virtuale per la scansione di immagini diagnostiche e delle radiografie, impiego di agenti robotici, utilizzo dei sistemi di linguaggio naturale per sottoporre ai pazienti specifici questionari precedenti al ricovero, fino alla predisposizione di *chatbot* riproducenti la figura del medico-ologramma sul modello della "S.A.R.A.H", di recente sviluppata dall'OMS[8]. Infine, l'IA è anche alla base di tutta quella vasta gamma di applicazioni installabili sul cellulare, in grado di identificare le componenti dei prodotti della consumazione, di predire il numero di calorie e di fornire raccomandazioni *ad hoc*, anche attraverso dispositivi *hi-tech* "indossabili"[9].

mantenimento e alla cura della salute fisica e psichica della persona. Al suo interno si esplicano le attività degli ospedali, degli ambulatori, delle strutture di cura sia pubbliche che private e delle strutture di ricerca e formazione.

[4] Ancora ai sensi della proposta della Commissione, il termine intelligenza artificiale «indica una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali». Torneremo *infra* sulla sua definizione giuridica definitiva.

[5] Si v. estensivamente sul punto A. Bohr, K. Memarzadeh (eds.), *Artificial Intelligence in Healthcare*, Amsterdam, 2020.

[6] Si v. R. Calvara, *Cosa pensa il Garante privacy italiano dell'uso dell'Intelligenza artificiale nel settore sanitario?*, in *Osservatorio sullo Stato digitale*, 29 novembre 2023; C. Di Costanzo, *L'impiego delle nuove tecnologie nel settore della salute: problematiche e prospettive di diritto costituzionale*, in *Consulta Online*, 2023, p. 214 ss.

[7] Partendo dallo sfruttamento di algoritmi sino alla creazione delle reti neurali profonde utilizzate per i modelli di *deep learning*. Si v. sul tema P. Traverso, *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE online*, n. 1, 2022, p. 155 ss.

[8] www.who-en.digitalhero.cloud/landing/index.html.

[9] In inglese, *wearable devices*, su cui S. Gilbert et al., *Citizen data sovereignty is key to wearables and wellness data reuse for the common good*, in *NPJ Digital Medicine*, n. 27, 2024, p. 27.

Sebbene tutti questi sistemi siano molto diversi tra loro, per tipologia, per uso e per grado di complessità tecnica, essi sono, per volontà del nuovo regolamento, tutti accomunati dall'impiego di un «sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[10] e quindi assoggettati alle norme del regolamento IA.

Esso guarda a questi sistemi con favore, a fronte delle riconosciute potenzialità di incremento della qualità della vita delle persone che il loro impiego comporta[11]. D'altra parte, il legislatore UE tenta però anche di regolare, mitigandoli *in nuce*, i rischi provenienti dalla loro comprovata e strutturale «opacità, complessità, dipendenza dai dati …e capacità di produrre un comportamento autonomo»[12].

Il regolamento, inoltre, ammettendo l'impiego di questi sistemi in un settore sensibile come quello della salute, assume una sicura rilevanza costituzionale[13]. Questi sistemi tecnologicamente avanzati sono infatti destinati ad avere un impatto elevato sugli assi portanti del diritto alla salute, per come declinato nel diritto interno[14] e nel diritto sovranazionale[15]. Poiché essi influenzeranno l'accesso alle cure e la loro qualità[16], nonché la tutela del diritto fondamentale alla protezione dei dati personali[17]. Lo stesso prin-

[10] Art. 3, par. 1, del regolamento IA, cit.

[11] M. Da Silva, T. Horsley et al., *Legal concerns in health-related artificial intelligence: a scoping review protocol*, in *Systematic Reviews*, n. 11, 2022, p. 123 ss.

[12] C. Schepisi, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *I Post di AISDUE*, n. 16, 2022, p. 330.

[13] Sul tema si v. G. Di Federico, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in C. Bottari (a cura di), *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, 2020, p. 17 ss.

[14] C. Di Costanzo, *L'impiego delle nuove tecnologie nel settore della salute*, cit., p. 216.

[15] G. Di Federico, S. Negri, *Unione europea e salute. Principi, azioni, diritti e sicurezza*, Padova, 2019.

[16] C. Di Costanzo, *Access to Intensive and Artificial Intelligence. A Constitutional Perspective*, in *Italian Journal of Public Law*, 2021, p. 594 ss.

[17] Declinato sia alla luce della disciplina del regolamento sulla protezione dei dati personali (GDPR), sia alla luce delle norme di diritto interno che codificano le regole deontologiche volte a regolare il rapporto di fiducia e confidenzialità tra medico e paziente, in cui rileva un simile, ma diverso "consenso informato" al trattamento rispetto a quanto regolato dal GDPR. Sul punto si v. D. Morana, T. Balduzzi, F. Morganti, *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *federalismi.it*, n. 34, 2022, p. 127 ss.

cipio di non discriminazione rischia di essere compromesso dall'impiego di sistemi di IA addestrati su dati che incamerino antichi e profondi pregiudizi culturali[18].

Quest'indagine intende analizzare come il nuovo regolamento classifichi e disciplini i vari sistemi di IA utilizzabili in ambito sanitario, e come tenti di risolvere alcune delle problematiche di ordine costituzionale appena accennate. A seguito di questa prima generale disamina, ci soffermeremo sulla coerenza del nuovo quadro regolatorio con la legislazione esistente al livello dell'Unione e con quella attualmente in discussione. Da ultimo, tenteremo di mettere l'accento sulle modalità e sull'efficacia dell'approccio regolatorio prescelto e sulla sua capacità di garantire un livello elevato di protezione della salute[19].

2. *I sistemi di IA impiegati in ambito sanitario e gli obblighi per i sistemi c.d. "ad alto rischio"*

Per prima cosa il regolamento definisce il suo oggetto e il suo ambito di applicazione. Esso, come anticipato, si applica a un gran numero di tecnologie, data l'ampissima definizione della nozione di «sistemi di IA» che novella[20]. Questa scelta, pur molto criticata dalla dottrina[21], va invero ponderata con la limitata struttura normativa del regolamento, basata sul c.d. *risk based approach*[22]. Essa finisce per regolamentare in maniera eteronoma e completa[23] solo i sistemi ritenuti davvero rischiosi. Fuori dalle applicazioni c.d. "ad

[18] È questo un dibattito molto presente nel mondo anglosassone e in particolare statunitense, su cui R. R. Fletcher, A. Nakeshimana, O. Olubeko, *Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health*, in *Frontiers in artificial intelligence*, vol. 3, 2021, p. 1 ss.

[19] Ovvero uno degli scopi del regolamento iscritti al considerando n. 1.

[20] Art. 3, punto 1, del regolamento IA.

[21] Si v. per una ricostruzione delle posizioni a favore e a sfavore di una definizione così ampia di questa nozione, C. T. Castán, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal*, n. 1, 2024, p. 305 ss.

[22] G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, 2022, p. 488 ss.; G. Finocchiaro, *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *La via europea per l'Intelligenza Artificiale*, 2022, p. 215 ss.; C. Quelle, *Enhancing compliance under the general data protection regulation: the risky upshot of the accountability-and risk-based approach*, in *European Journal of Risk Regulation*, n. 3, 2018, p. 502 ss.

[23] Ovvero i caratteri della "normatività", per cui si rimanda all'intramontabile categoriz-

alto rischio" e di alcuni sistemi di IA per finalità generali, infatti, il regolamento non impone obblighi normativamente vincolanti[24]. Ciò restringe non la portata stessa del regolamento, ma quella delle sue singole disposizioni e, in particolare, di quelle che pongono obblighi vincolanti.

Nella delimitazione del suo ambito di applicazione, il regolamento chiarisce anche che non si applica ai sistemi di IA usati «esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività, nonché alle attività di ricerca, sviluppo e prototipazione che precedono l'immissione sul mercato o a persone che utilizzano l'IA per motivi non professionali»[25]. L'esclusione delle attività di ricerca è ribadita all'art. 1, par. 8 del regolamento, ai sensi del quale esso non si applica «alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio».

Questa esclusione, che toccherà da vicino le attività dei dipartimenti di ricerca e sviluppo dei nuovi prodotti, servizi ed app pensate per il settore medico, si ispira a quanto già avviene per la messa in commercio di nuovi farmaci, ove è solo il prodotto finale, già pronto per essere commercializzato, a essere oggetto di specifica regolazione[26]. Di conseguenza, le tecnologie di IA sviluppate dai dipartimenti di ricerca e sviluppo delle case farmaceutiche o dalle industrie della salute e del benessere risultano al momento prive di apposita regolamentazione sovranazionale. Esse potranno dunque essere disciplinate dal legislatore nazionale fintanto che questo "spazio" di normazione concorrente[27] non venga "occupato" dal legislatore dell'Unione.

L'obiettivo del regolamento è, come noto, di natura principalmente economica, volto cioè alla costituzione di un mercato unico per lo scambio e l'utilizzo di sistemi di intelligenza artificiale affidabili, da impiegare però nel rispetto dei valori e dei diritti fondamentali dell'UE[28]. Questo rispetto passa,

zazione di V. Crisafulli, *Atto normativo*, in *Enciclopedia del diritto*, vol. IV, 1959, p. 238 ss.

[24] Ma suggerisce l'adozione di regole di auto-condotta. Simoncini e Cremona ritengono si tratti di un «modello di etero-regolazione combinato con un modello di co-regolazione debole», in A. Simoncini, E. Cremona, *La AI fra pubblico e privato*, in *DPCE online*, n. 1, 2022, p. 260.

[25] Art. 2, par. 3, regolamento IA.

[26] L. Nottage, *Product safety regulation*, in AA.VV., *Handbook of Research on International Consumer Law*, Cheltenham, 2018, p. 231 ss.

[27] Indicata dalla scelta della base giuridica preminente del regolamento IA e cioè l'art. 114 TFUE, su cui si v. M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in questo *fascicolo speciale*, pp. 12-13.

[28] A. Adinolfi, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e*

in particolare, attraverso la protezione di «un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea»[29].

Questo tentativo di contemperamento rispecchia la tecnica legislativa prescelta: quella di coniugare un approccio "classico" alla normazione, limitato a riprodurre quanto già esistente nella legislazione verticale sulla circolazione e sicurezza dei prodotti[30], con un approccio "nuovo" o "creativo", che si preoccupa di superare la logica del mercato mettendo in risalto considerazioni relative alla protezione dei diritti fondamentali, così come dei processi democratici e dello Stato di diritto[31].

Per mettere in comunicazione questi due diversi approcci, il regolamento predilige il già menzionato sistema di classificazione proporzionale del rischio, su cui graduare, con diverse intensità, numerosi obblighi tecnico-giuridici gravanti sia sugli «operatori» dei sistemi di IA, sia sugli «utilizzatori» (siano pubbliche amministrazioni o persone fisiche e giuridiche di natura privata)[32], nonché sugli Stati membri.

Sulla base di tale sistema di classificazione, i sistemi ad alto rischio saranno sottoposti a obblighi più gravosi, mentre quelli a rischio lieve o minimo a meri obblighi di auto-condotta[33]. Se così stanno le cose, la concreta efficacia del regolamento si giocherà tutta sulla corretta identificazione della classe di rischio e dei conseguenti obblighi, di natura eventualmente vincolante, scaturenti da tale classificazione[34].

sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione, in AA. VV., *Intelligenza artificiale e diritto: una rivoluzione*?, Bologna, 2022, p. 127 ss.

[29] Considerando n. 1 del regolamento IA.

[30] Una sorta di "vecchio nuovo approccio" per cui si v. S. De Vries, O. Kanevskaia, R. De Jager, *Internal Market 3.0: The "Old" New Approach for Harmonising AI Regulation*, in *EP*, n. 2, 2023, p. 583 ss.; S. De Vries, *Recent trends in eu internal market legislation. Bringing back the old concepts?*, in T. Van Den Brink, V. Passalacqua (eds.), *Balancing unity and diversity in EU legislation*, Cheltenham, 2024, p. 17 ss.

[31] Questi due approcci sono evidenti in tutto il pacchetto UE per la digitalizzazione e quindi anche nel DMA e soprattutto nel DSA. Per quanto riguarda il regolamento IA, si v. l'intervista a Roberto Viola, reperibile qui. Sul punto anche F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in questo *fascicolo speciale*, p. 1 ss.

[32] Torneremo *infra* su queste due nozioni.

[33] J. Black, *Decentring Regulation: Understanding the Role of Regulation and Self-regulation in "Post-Regulatory" Word*, in *Current Legal Problems*, n. 1, 2001, p. 112 ss.

[34] La classificazione e gli obblighi "spalmati" sulle diverse classi non appaiono pertanto poi così proporzionali poiché questa gradazione si muove solo su due poli, peraltro collocati

Prima però di entrare nel cuore di questa questione[35], occorre menzionare la categoria del rischio «inaccettabile», vietato dal regolamento[36].

Infatti, solo i sistemi il cui rischio, finanche molto alto, sia comunque considerato «accettabile» potranno circolare nel mercato unico. Viceversa, quando il rischio frutto dell'uso di quel sistema sia ritenuto inaccettabile, ad esempio perché tale da mettere a rischio la vita della persona, sarà completamente bandito dal mercato, con conseguente illiceità del suo utilizzo[37]. Inaccettabile non è dunque mai il sistema di IA in sé per sé, bensì il suo utilizzo o, meglio, «le pratiche» eccessivamente rischiose a cui esso può prestarsi.

Tra le pratiche vietate figurano, in particolare, l'identificazione biometrica remota in tempo reale, la lettura delle emozioni in base ai dati biometrici, l'uso di tecniche subliminali, la previsione dei reati o il c.d. *social scoring*. Tra queste, nessuna esclusione pertiene direttamente all'ambito sanitario[38]. Anzi, «motivi medici», presumibilmente di ordine psichiatrico o «di sicurezza», costituiscono deroghe al divieto posto all'art. 5, lett. *f)* in merito all'immissione sul mercato o alla messa in servizio dell'uso di sistemi di IA volti a inferire le emozioni di una persona nell'ambito del luogo di lavoro e degli istituti di istruzione.

Tuttavia, l'art. 5, par. 1, lett. *b)*, vieta «la messa in servizio o l'uso di un sistema di IA che sfrutta le *vulnerabilità* di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla *disabilità* o a una *specifica situazione sociale o economica*, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo»[39]. Nella nozione di «danno significativo» dovrebbe certamente rientrare il danno alla salute, mentre il «gruppo vulnerabile» potrebbe ragionevolmente essere identificato con quello dei pazienti affetti da una stessa patologia. Stando a questa

apparentemente ai due estremi opposti. Tralasciamo qui però la categoria dei sistemi di IA per finalità generali, in parte assimilati ai sistemi ad alto rischio.

[35] Che riguarda da vicino proprio i sistemi di IA applicabili in ambito sanitario che, come vedremo, dovrebbero per la maggior parte confluire nella classe di rischio più elevata. Da un lato perché essi saranno presumibilmente usati a fini diagnostici e terapeutici e saranno classificati come dispositivi medici, dall'altro in ragione dell'eventuale impatto che possono avere sulla sicurezza fisica delle persone e sui loro diritti fondamentali.

[36] La rappresentazione figurativa dell'approccio basato sul rischio è infatti quella di una piramide, la cui punta è costituita dal rischio inaccettabile e la base dal rischio nullo.

[37] Art. 5 del regolamento IA.

[38] *Ibidem*.

[39] Corsivo aggiunto.

lettura, è possibile immaginare che in futuro alcuni impieghi delle tecnologie basate sull'IA saranno bandite in ambito sanitario.

In tal senso soccorre il considerando n. 58 del regolamento, il quale, pur riferendosi ad alcuni degli usi da considerarsi ad alto rischio, annovera coloro che «ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, *vale a dire servizi sanitari*, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia (…)» tra le persone che «si trovano generalmente in una *posizione vulnerabile* rispetto alle autorità responsabili».[40]

Scendendo di un livello la piramide raffigurante l'approccio basato sul rischio, il regolamento definisce la classificazione dei sistemi ad alto rischio. È in questa classe che confluiranno molte delle tecnologie utilizzabili in ambito sanitario e ciò essenzialmente per due ordini di ragioni: la destinazione d'uso, eventualmente a fini diagnostici e terapeutici della tecnologia, e la sua qualificazione come dispositivo medico.

In particolare, riguardo al primo aspetto, sono considerati ad alto rischio, in ragione del loro uso:

a) «i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per *valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali*, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;

(….)

d) i sistemi di IA destinati a essere utilizzati *per valutare e classificare le chiamate di emergenza* effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco *e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza*»[41].

A proposito di queste diverse fattispecie menzionate dall'Allegato III del regolamento, vale la pena sottolineare il diverso ambito soggettivo delle disposizioni regolamentate alla lett. *a)*, la quale si rivolge espressamente alle autorità pubbliche o ad autorità private che operano per conto di autorità pubbliche, ovvero che siano oggetto di delega di poteri pubblici, e alla lett. *d)* la quale, invece, non menziona la natura

[40] Corsivo aggiunto.

[41] Punto 1, Allegato III, del regolameno IA (corsivo aggiunto).

pubblica o privata dell'ente ma solo la tipologia di servizio: l'assistenza sanitaria di emergenza, indipendentemente dalla natura del soggetto erogatore[42].

La diversa definizione dei sistemi ad alto rischio, basata, in un caso, sulla natura pubblica del prestatore e, nell'altro, sulla tipologia del servizio erogato, si spiega alla luce di vari ordini di ragioni. In primo luogo, nella maggior parte dei sistemi costituzionali degli Stati membri, è l'autorità pubblica che, in applicazione del fondamentale principio di solidarietà sociale, ha l'obbligo di assicurare l'erogazione di un efficiente servizio sanitario nazionale per i suoi cittadini[43], indipendentemente dalle modalità del suo finanziamento.

Inoltre, nella misura in cui il regolamento IA adotta un "approccio antropocentrico"[44], una tecnologia potenzialmente «disruptive»[45] dovrebbe sempre essere posta sotto la supervisione umana. L'essere umano è infatti l'unico agente in grado di effettuare una scelta "ragionevolmente orientata" a tutela dei diritti e della libertà delle persone, e quindi, ancor prima, della loro vita. Ciò è particolarmente rilevante nel caso dei servizi di urgenza, in cui la protezione di questo bene primario è richiesta a qualunque prestatore.

Infine, non rilevano né la natura giuridica dell'agente umano, in quanto il titolare degli obblighi può essere una persona fisica o giuridica, né, in questo ultimo caso, quella pubblica o privata. Conta, invece, la qualificazione oggettiva dell'attività erogata, che deve essere riconducibile a un "servizio essenziale". Questo profilo, come giustamente notato, rivela una "concezione funzionale di servizio essenziale", che ne valorizza il ruolo sociale, indipendentemente dal fatto che ad erogarlo sia un soggetto pubblico o uno privato, con conseguente «responsabilizzazione dei grandi player privati dell'era digitale»[46].

Sulla base di quanto esposto, ai sensi del regolamento IA, gli stessi identici programmi statistici e di linguaggio naturale usati per stabilire i turni dei medici e degli infermieri nelle strutture ospedaliere –generalmente conside-

[42] Sul tema, O. M. Puigpelat, *The impact of the AI Act on public authorities and on administrative procedures*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, vol. 4, 2023, p. 238 ss.

[43] V. Salvatore, *Il diritto alla salute. Una prospettiva di diritto comparato*, in *EPRS Servizio ricerca del Parlamento europeo*, 2021.

[44] Comunicazione della Commissione europea, Creare fiducia nell'intelligenza artificiale antropocentrica, COM (2019) 168final, dell'8 aprile 2019.

[45] R. Girasa, *Artificial intelligence as a disruptive technology: Economic transformation and government regulation*, Berlin, 2020.

[46] A. Simoncini, E. Cremona, *op. cit.*, pp. 259-260.

rati a rischio lieve o nullo – non potranno essere impiegati per determinare le preferenze di accesso in ospedale[47].

Dietro questa logica si annida l'idea della "neutralità" della tecnologia dal punto di vista del suo trattamento giuridico. Conformemente a tale logica, non è il programma in sé per sé a causare l'eventuale violazione dei diritti fondamentali, ma il suo specifico uso ragion per cui il programma può essere liberamente sviluppato da coloro che hanno gli strumenti e la conoscenza tecnica per farlo. Anzi, vi è un evidente incentivo allo sviluppo, dacché la sua presunta neutralità iniziale ripara il programma da eventuali illeciti, ponendolo invece in corsa verso uno sviluppo sempre più avanzato. Al contempo, però, ai sensi del regolamento, tale presunta iniziale neutralità retrocede in casi specificatamente determinati e, in particolare, dinanzi alla necessità di proteggere i diritti e le libertà delle persone che potrebbero essere degradati dall'uso concreto di tale tecnologia[48]. Ciò può accadere nel caso in cui il sistema di IA sia concretamente impiegato in settori sensibili, come quello della sanità, che hanno a che vedere con la tutela della vita, con il suo miglioramento e, più in generale, con l'inclusione di tutti i cittadini indipendentemente dalla loro classe socioeconomico e culturale.

I c.d. sistemi ad alto rischio, però, non sono solo definiti in base a questo criterio "d'uso", volto a valorizzare i rischi concreti dell'applicazione di tecnologie presuntivamente neutre. L'art. 6 posto nel corpo del regolamento[49] menziona anzitutto i sistemi considerati ad alto rischio, perché coperti da una normativa di armonizzazione dell'UE[50]. Un sistema di IA sarà in base a tale disposizione considerato ad alto rischio quando soddisfa due condizioni cumulative:

a) «è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul

[47] Evidentemente qui il rischio è quello di una discriminazione di alcuni individui o gruppi sociali.

[48] Ovvero in un certo contesto, in uno specifico settore e rispetto a una determinata categoria di soggetti.

[49] E quindi non in un Allegato.

[50] Da questo punto di vista anche qui vi è una integrazione tra un approccio "innovativo" o "antropocentrico" e un approccio "classico" ovvero obiettivo.

mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I».

Tra le normative di armonizzazione più rilevanti per il nostro ambito figurano: il regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio; il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE ; il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio; e il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE; la decisione 2010/227/UE della Commissione[51].

In base ai regolamenti sui dispositivi medici, sono ad alto rischio tutti i dispositivi medici e i dispositivi medico-diagnostici che rientrano nelle classi IIa, IIb o III e che sono, pertanto, sottoposti a una procedura di valutazione della conformità da parte di un organismo terzo, ai sensi del regolamento (UE) n. 2017/745[52]. Quelli collocati nella prima classe di rischio disciplinata da tale regolamento, viceversa, sono solo sottoposti a un'auto-valutazione, senza il coinvolgimento di un organismo indipendente, come disposto anche dal regolamento IA[53]. Quest'ultimo, infatti, stabilisce che, se non è previsto, dalla legislazione settoriale, il coinvolgimento di un organismo qualificato, la valutazione della conformità deve essere fatta in base «al controllo interno di cui all'Allegato VI» del regolamento[54]. Di tal fatta, la struttura della procedura di valutazione della conformità, stabilita nei due regolamenti, resta sostanzialmente la stessa[55].

Sono allora due i meccanismi di classificazione dei sistemi ad alto rischio. Il primo mette in risalto l'uso concreto o la pratica concreta del sistema, sposando così un approccio decisamente "innovativo" alla regolazione, che guarda alla tecnologia come neutra in astratto ma da supervisionare in

[51] A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in questo *fascicolo speciale*, p. 1 ss.

[52] Allegato VIII del regolamento (UE) n. 2017/745, cit., il quale stabilisce regole di classificazione basate sulla destinazione d'uso medico.

[53] Sul punto A. Kiseleva, *AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation*, In *Time to Reshape the Digital Society. 40th Anniversary of the CRIDS*, Namur-Belgium, November 2021.

[54] Art. 43, par. 1, lett.) *a*.

[55] A. Volpato, *op. cit*.

concreto. Il secondo, viceversa, è basato sulle norme di armonizzazione ed è riconducibile nell'alveo di quell'approccio normativo da noi definito "classico", che si limita a riprodurre la logica già sperimentata in materia di circolazione e sicurezza dei prodotti. I due approcci sono destinati ad integrarsi e contemperarsi, a condizione che il regolamento IA assuma la funzione di "modello" nel quale è richiamata la struttura della legislazione verticale già esistente, la cui portata viene però estesa in ragione della valorizzazione di considerazioni di più ampia portata e di carattere sociale.

Ad esempio, in base al regolamento sui dispositivi medici, poiché rileva la destinazione d'uso dichiarata, i sistemi IA di monitoraggio o che forniscono consigli su come migliorare lo stato di salute (come è talvolta il caso dei dispositivi indossabili), non dovrebbero essere considerati «dispositivi medici», in base a quanto suggerito dal considerando n. 19 del suddetto regolamento[56] e, di conseguenza, non dovrebbero rientrare nella categoria dell'«alto rischio» prevista dal regolamento IA.

Viceversa, i sistemi volti a monitorare i livelli di serotonina per determinare la reazione del paziente alle cure – normalmente usati per finalità diagnostiche e terapeutiche – dovrebbero, ai sensi dell'art. 2, par. 1, del regolamento sui dispositivi medici e della regola n. 11 ivi stabilita, essere considerati «accessori di un dispositivo medico» e quindi rientrare nella classe IIa[57]. Di conseguenza essi saranno classificati come ad alto rischio, ai sensi del regolamento IA.

Tuttavia, questi metodi di classificazione non sono così rigidi e potrebbero, nell'applicazione pratica, essere neutralizzati in virtù delle numerose deroghe introdotte nei successivi paragrafi dell'art. 6 del regolamento IA[58]. Queste deroghe permettono una mutazione della classe di rischio che potrebbe prodursi sia in presenza di un sistema di IA considerato ad alto ri-

[56] Ai sensi del quale: «il software specificamente destinato dal fabbricante a essere impiegato per una o più delle destinazioni d'uso mediche indicate nella definizione di dispositivo medico si considera un dispositivo medico, mentre il software destinato a finalità generali, anche se utilizzato in un contesto sanitario, o il software per fini associati allo stile di vita e al benessere non è un dispositivo medico. La qualifica di software, sia come dispositivo sia come accessorio, è indipendente dall'ubicazione del software o dal tipo di interconnessione tra il software e un dispositivo».

[57] J. Van Oirschot, G. Ooms, *Interpreting the EU Artificial Intelligence Act for the Health Sector*, Amsterdam, 2022, p. 10.

[58] Ciò che permette che un sistema di IA che rientra nell'allegato III non sia considerato ad alto rischio qualora non presenti «un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, *anche* nel senso di non influenzare materialmente il risultato del processo decisionale».

schio in virtù dell'Allegato III, sia quando si tratti di un sistema di IA non ad alto rischio che successivamente venga integrato in tale allegato in base al suo uso concreto[59].

Nel primo caso il sistema di IA astrattamente ad alto rischio potrebbe essere considerato concretamente non in grado di influenzare il risultato del processo decisionale e dunque essere escluso dai sistemi ad alto rischio in applicazione dell'art. 6, par. 3 del regolamento, poichè, ad esempio, è «destinato a migliorare il risultato di un'attività umana precedentemente completata»[60]. In questo caso, il fornitore effettua una auto-valutazione che dovrà eventualmente essere presentata alle autorità nazionali competenti su loro richiesta[61]. Ai sensi dello stesso articolo, il fornitore è inoltre soggetto all'obbligo di registrazione di cui all'articolo 49, par. 2, del regolamento.

Nel secondo caso, potrebbe trattarsi ad esempio di un'applicazione per il benessere che archivia dati di soggetti affetti da particolari disturbi psichici o che monitora il flusso mestruale delle donne e che, non qualificata come dispositivo medico, dovrebbe essere considerata a rischio lieve. Tuttavia, lo stesso dispositivo potrebbe essere successivamente ricondotto, magari per qualche ragione geopolitica, tra i sistemi ad alto rischio, in virtù di una modifica dell'allegato III inserita *ex post* dalla Commissione[62]. Queste considerazioni valgono in particolare per i c.d. «sistemi indipendenti» o *stand alone* che, non essendo componenti di prodotti dei dispositivi medici, sono assoggettati a procedure di auto-valutazione effettuate dallo stesso fornitore.

Avendo sommariamente delineato il sistema di definizione della classe ad alto rischio e le ragioni per le quali interessa da vicino i modelli di IA utilizzati in ambito sanitario, occorre ora analizzare gli obblighi più stringenti gravanti sugli operatori dei sistemi ad alto rischio.

Tali obblighi sono disciplinati dal Capo II del regolamento, il quale fa riferimento a doveri più specifici di trasparenza, accuratezza, robustezza e cibersicurezza e alla tutela dei diritti fondamentali[63]. Anzitutto, la documen-

[59] Le mutazioni delle classi di rischio sono quindi più facilmente realizzabili per i sistemi "indipendenti" o c.d. *stand-alone*.

[60] In applicazione dell'art. 6, par. 3, lett. *b)*, del regolamento IA.

[61] *Ibidem*, art. 3, par. 4.

[62] Su cui F. Ferri, *op. cit*., p. 4 ss. Per alcune considerazioni sul binomio geopolitica e salute si v. risoluzione del Parlamento europeo, del 20 gennaio 2021, sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)).

[63] Art. 8 del regolamento IA.

tazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio e deve essere tenuta aggiornata nel tempo[64]. Se già prevista dalle norme di armonizzazione, essa sarà unica e integrerà gli obblighi delle diverse normative al fine di diminuire i costi e gli oneri gravanti su fornitori e produttori.

Lo stesso vale per la «valutazione della conformità» imposta ai sensi dell'art. 43 e per la marcatura CE, già prevista ai sensi della legislazione sulla commercializzazione e la sicurezza di alcuni prodotti[65]. Come anticipato, la valutazione della conformità diventa però una sorta di auto-valutazione, nel caso dei c.d. sistemi indipendenti che non sono classificati né come prodotti, né come componenti di sicurezza di un prodotto[66].

Per tutti i sistemi ad alto rischio, poi, occorre prevedere un sistema di gestione dei rischi ai sensi dell'art. 9 al fine di assicurare un aggiornamento costante e sistematico agli obblighi imposti. Inoltre, un obbligo di monitoraggio successivo all'immissione nel mercato è disciplinato all'art. 72 del regolamento.

Sono questi tutti obblighi che ci paiono essenzialmente di carattere procedurale. A questi si aggiungono però anche obblighi che potremmo definire sostanziali, quali gli obblighi di «trasparenza e fornitura di informazioni ai deployer» previsti ai sensi dell'art. 13. Quest'obbligo di trasparenza, corollario del c.d. «diritto alla spiegabilità», derivato dalla giurisprudenza sull'art. 22 del GDPR, è preposto allo scopo di rendere comprensibile il funzionamento del sistema, al fine di ingenerare un utilizzo – ed eventualmente un consenso all'utilizzo –consapevole. Quest'obbligo diviene "sostanziale" se e nella misura in cui è associato al c.d. diritto ad ottenere la spiegazione dei singoli processi decisionali ai sensi del GDPR[67].

Quest'obbligo di trasparenza declinato in senso sostanziale è assai diverso da quello previsto dall'art. 52 del regolamento IA, che si applica ad alcuni sistemi di IA per finalità generali, come le c.d. *chat boxes*. In questo caso, si richiede solo di rendere noto all'utente il fatto che si stia

[64] *Ibidem*, art. 11.

[65] Decisione (UE) n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti.

[66] Questi seguono le regole iscritte nell'Allegato VI ed eventualmente VII.

[67] Sul punto, G. Contaldi, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, pp. 1210-1211.

interagendo con un sistema di IA, ragion per cui esso, più che un vero e proprio obbligo di trasparenza, dovrebbe rappresentare un obbligo informativo[68].

Particolare attenzione merita la c.d. valutazione di impatto sui diritti fondamentali (FRIA)[69]. Questa è stata fortemente voluta dal Parlamento europeo[70], il quale ha rafforzato la proposta avanzata dal Consiglio in sede di trilogo, la quale richiedeva ai *deployer* dei sistemi di IA ad alto rischio solo di prevedere e analizzare *ex ante* una lista di rischi potenziali per la salute, la sicurezza e i diritti fondamentali. Secondo la modifica voluta dal Parlamento europeo[71], ora confluita nell'art. 27 del regolamento, l'attuale FRIA, acronimo dell'inglese *fundamental rights impact assessment*, non si riduce a un mero elenco *ex ante* dei possibili rischi, ma tenta di coadiuvare anche una previsione *ex post* relativa all'uso concreto dei sistemi di IA[72]. Per far ciò prevede una serie di obblighi aggiuntivi per i *deployer* dei sistemi di IA, considerati «nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili»[73].

I *deployer* obbligati dalla FRIA sono solo gli organismi di diritto pubblico o enti privati che forniscono servizi pubblici, ovvero *deployer* di sistemi di IA ad alto rischio, di cui all'allegato III, punto 5, lett. *b)* e lett. *c)*. Questi devono redigere una valutazione in cui vengano descritte le applicazioni del sistema ad alto rischio, il periodo di tempo e la frequenza di tale utilizzo, le

[68] A. Kiseleva, *Making ai's transparency transparent: notes on the EU proposal for the Ai Act*, in *European Law Blog*, 2021; e anche 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 *Frontiers in artificial intelligence*, 2022, p. 1 ss.

[69] J. Mökander, M. Axente, F. Casolari, L. Floridi, *Conformity assessments and post-market monitoring: a guide to the role of auditing in the pro-posed European AI Regulation*, in *Minds and Machines*, vol. 32, 2021, p. 1 ss.

[70] www.eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52023AP0236.

[71] Su cui si v. anche E. Cirone, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in questo *fascicolo speciale*, p. 14.

[72] Poiché in base considerando n. 58 *bis* introdotto dall'emendamento del Parlamento (ora considerando n. 93): «Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche *dal modo in cui tali sistemi di IA sono utilizzati*».

[73] Considerando n. 93 del regolamento IA.

categorie di persone fisiche e dei gruppi che possono essere interessati dal suo uso, i rischi specifici di danno che possono incidere su determinati gruppi o categorie di persone (minoranze, gruppi vulnerabili) e, infine, le misure di sorveglianza umana[74] e di rimedio alla concretizzazione dei rischi[75].

Di tutti gli obblighi che abbiamo citato, solo gli ultimi due gravano però sul *deployer*, mentre i primi gravano sul "fornitore". A riguardo, giova ricordare che, ai sensi dell'art. 1, par. 2, lett. *c)*, il regolamento stabilisce «requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi». La nozione di operatore e assai ampia. e include, ai sensi dell'art. 3, par. 8, «un fornitore, un fabbricante del prodotto, un *deployer*, un rappresentante autorizzato, un importatore o un distributore», laddove, in particolare, un fornitore è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito»; mentre un *deployer* è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

In base all'art. 25, la nozione di "fornitore" è aperta, poiché si può diventare fornitori al verificarsi di una delle condizioni indicate dall'articolo in questione. Inoltre, le figure del *deployer* e del fornitore potrebbero anche sovrapporsi, in virtù dell'applicazione congiunta delle regole previste dal regolamento IA, in particolare quelle relative all'obbligo di adottare idonee misure tecniche e organizzative[76], e di quelle del regolamento sulla protezione dei dati, il quale ammette la possibilità di una contitolarità di obblighi[77].

[74] In raccordo con l'art. 14 e il principio della c.d. «non esclusività della decisione algoritmica».

[75] Inoltre, l'operatore che è un'autorità pubblica o un'impresa di cui all'articolo 51, par. 1 *bis*, lett. *b)*, pubblica una sintesi dei risultati della valutazione d'impatto nell'ambito della registrazione dell'uso ai sensi dell'obbligo di cui all'articolo 51, par. 2.

[76] *Ibidem*, art. 70.

[77] Sul punto G. Contaldi, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in P. Manzini, G. Contaldi, G. Caggiano (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, p. 207 ss.

3. *Il problema della coerenza con altri strumenti legislativi*

È questo uno dei tanti aspetti che riguarda il più generale problema della c.d. «coerenza con le disposizioni vigenti nel settore normativo interessato»[78]. Il problema della coerenza si pone in maniera diversa in base alla tipologia della legislazione con cui il regolamento si confronta, sia essa verticale oppure trasversale.

3.1. Segue*: la coerenza con la legislazione verticale*

Il regolamento ha tentato di preservare la massima coerenza con le legislazioni verticali adoperando la tecnica del rinvio, la quale consente una vera e propria integrazione delle regole previste dal regolamento IA con le varie e assai complesse normative settoriali richiamate nel corpo del testo, nei considerando e negli appositi allegati[79].

Si pensi alla procedura di valutazione della conformità dei prodotti dei quali un sistema di IA costituisce una componente di sicurezza, o a quelle nelle quali il sistema di IA in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio. In simili casi, l'articolo 43 del regolamento IA rinvia alle diverse normative di armonizzazione elencate nell'allegato I del regolamento stesso[80], assicurando la massima coerenza. Un sistema di IA potrà circolare nel mercato dell'UE solo se già risulta conforme a tutta la normativa di armonizzazione dell'Unione che gli è astrattamente applicabile[81].

Se in astratto questa "coerenza" è ottenuta tramite la tecnica del rinvio, il quale permette l'integrazione della normativa settoriale rinviata nella legislazione rinviante[82], nella pratica ciò consente anche di evitare la duplicazione di sforzi "amministrativi" o "burocratici" già inscritti nelle legislazioni precedenti e che potrebbero risultare particolarmente onerosi per le piccole

[78] Si v. ancora COM (2021) 206final, cit.

[79] Sono ancora in corso di adozione le normative relative «ai requisiti essenziali di cibersicurezza di un prodotto» e ai «prodotti con elementi digitali critici».

[80] Su questo ampiamente A. VOLPATO, *op. cit*.

[81] Ai sensi del considerando n. 46, il regolamento si applica «senza pregiudizio» di tali normative.

[82] Viceversa, come giustamente si sottolinea al considerando n. 124: «L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica, la metodologia o la struttura generale specifiche della valutazione della conformità a norma della pertinente normativa di armonizzazione dell'Unione».

e medie imprese. Ulteriori esempi di rinvio possono trovarsi negli obblighi di «marcatura CE», previsti dall'art. 48 del regolamento IA[83] e dall'art. 47, par. 3, che consentono di redigere un'unica dichiarazione di conformità per un prodotto già sottoposto ad altra normativa di armonizzazione.

3.2. Segue*: la coerenza con il GDPR*

Più difficoltosa appare la coerenza con le normative trasversali e in particolare con il GDPR[84]. Infatti, benché ai sensi del decimo considerando, «il presente regolamento non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti», vi sono diverse sovrapposizioni tra queste due normative, non sempre risolte dal legislatore[85].

Sebbene egli abbia in astratto pensato a un approccio di tipo complementare[86], è evidente che, nella pratica, le due normative non sono sempre facilmente conciliabili, ispirandosi a principi e interessi parzialmente diversi[87]. Poiché esse però indubbiamente interagiscono, in particolare nel caso di sistemi di IA utilizzati per fini diagnostici e terapeutici che si basino anche sui dati sensibili[88], occorre domandarsi come il regolamento risolva queste "sovrapposizioni", tenendo anche presente che il fornitore di un sistema di IA potrebbe essere al contempo il «titolare del trattamento» ai sensi del GDPR.

[83] Conformemente ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

[84] Il fatto che sia il regolamento IA, sia il GDPR siano norme di applicazione trasversale (in un caso all'uso dei sistemi di AI in tutti gli ambiti eccetto che in quelli espressamente esclusi e nel GDPR nel caso di un qualsiasi trattamento di dati personali) assicura tra loro molte probabili sovrapposizioni o «cumuli» in G. Contaldi, *Intelligenza artificiale e dati personali*, cit., p. 1203.

[85] E perciò probabilmente devolute a una risoluzione in via giudiziale.

[86] Su cui G. C. Feroni, *Intelligenza artificiale e ruolo della protezione dei dati personali*, 14 febbraio 2023, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742.

[87] Molto si è detto sulle «*tensions and proximities between AI and data protection principles, such as, in particular, purpose limitation and data minimisation*», in G. Sartor, F. Lagioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, EPRS_STU(2020)641530, 2020.

[88] Quest'uso è per altro doppio poiché: «*On the one hand, personal data may contribute to the data sets used to train machine learning systems, namely, to build their algorithmic models. On the other hand, such models can be applied to personal data, to make inferences concerning particular individuals*», in G. Sartor, F. Lagioia, *op. cit*.

Anzitutto, vi è parziale comunicazione tra i due atti rispetto all'obbligo di predisporre una valutazione d'impatto: sui diritti fondamentali ai sensi dell'art. 27 del regolamento IA e sulla protezione dei dati in base all'art. 35 del GDPR. Il par. 4 dell'art. 27 prevede che «se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati». Ciò dovrebbe consentire al *deployer* del sistema ad alto rischio di ottimizzare gli sforzi, di fatto mimando quanto già fatto durante il DPIA, ma allargando la valutazione sulla protezione dei dati personali ad altri diritti fondamentali[89].

Sul punto, però, non possono sottacersi alcune criticità. Anzitutto, come appena anticipato, le due valutazioni, benché condividano uno stesso intento, hanno ambiti di applicazione diversi. Quindi, la FRIA non potrà limitarsi a richiamare la valutazione di impatto sulla protezione dei dati personali, ma dovrà anche preoccuparsi di altri diritti come la sicurezza, la salute e il principio di non discriminazione; per tacere in questa sede degli eventuali «rischi sistemici»[90].

In secondo luogo, la DPIA è richiesta alle condizioni e nei casi menzionati ai parr. 1 e 3 dell'art. 35 del GDPR, che non necessariamente coincidono con le condizioni (soggettive) stabilite ai sensi del regolamento sull'intelligenza artificiale. Come messo precedentemente in evidenza, infatti, la FRIA è richiesta solo a una categoria particolare di *deployer*, che siano, cioè, soggetti pubblici o che eroghino prestazioni essenziali[91]. Per questo, sarebbe stato allora forse più opportuno estendere la FRIA a tutti i sistemi ad alto rischio, come inizialmente richiesto dal Parlamento europeo, oppure prevedere un esplicito sistema di raccordo con il GDPR, ampliando l'applicazione della FRIA per tutti i titolari di trattamento di dati particolarmente sensibili, quali quelli sanitari.

Al GDPR si ispirano anche le misure tecniche ed organizzative necessarie a garantire la sicurezza dei sistemi di IA, improntate sul principio della sicurezza fin dalla progettazione, inscritto nell'art. 25 del GDPR, del quale, nondimeno, non si fa espressa menzione nel regolamento IA. Quest'ulti-

[89] E che comprendono, in particolare, il diritto alla dignità, all'eguaglianza e alla non discriminazione, alla salute, ma anche ad alcuni diritti politici, come quelli alla libertà di espressione e all'elettorato passivo.

[90] Disciplinati dal regolamento.

[91] Si v. *supra*.

mo richiama però la "pseudonimizzazione" in quanto «misura avanzata di sicurezza per la vita privata», anche ai sensi dell'art. 10, par. 5, lett. *b)* del regolamento IA.

In ambito sanitario, l'eventuale sovrapposizione dei due regolamenti solleva anche il problema dell'utilizzo dei dati sanitari (ai sensi dell'art. 9 del GDPR)[92], nell'ambito di un sistema incentrato su «processi decisionali automatizzati» (ai sensi dell'art. 22, par. 1, del GDPR), eventualmente anche al fine della «profilazione» (art. 4, par. 4 e art. 22, par. 4) del paziente.

In questi casi, i principi del GDPR sono rafforzati. Quello della "liceità" richiede che una espressa base giuridica per il trattamento venga rinvenuta, se non nel consenso espresso degli interessati, nelle lettere *g)* o *i)* del secondo paragrafo dell'art. 9 del GDPR e cioè nei «motivi di interesse pubblico rilevante» o nei «motivi di interesse pubblico nel settore della sanità pubblica», i quali devono essere declinati sulla base del diritto dell'Unione o degli Stati membri. Questi ultimi, come noto, possono, ai sensi dell'ultimo paragrafo di questo articolo, porre «ulteriori limitazioni»[93].

L'intervento legislativo nazionale è auspicabile, secondo il «Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale», al fine di assicurare un trattamento compatibile con il GDPR allorquando si operi senza il consenso esplicito dell'interessato. Come previsto anche dall'art. 22, par. 4, del GDPR. Infatti, le decisioni automatizzate, inclusa la profilazione, non possono basarsi sul trattamento di dati relativi alla salute, a meno che i dati siano trattati per motivi di pubblico interesse. Questa stessa base giuridica, inoltre, sarebbe anche in linea con quanto auspicato dalla Dichiarazione sui diritti e principi digitali, proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione, nel 2023[94].

Questi motivi di interesse pubblico, però, non figurano espressamente nell'art. 10, par. 5 del regolamento IA, il quale consente ai fornitori l'utilizzo dei dati sensibili, inclusi quelli sanitari, «al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio»,

[92] Si tratterà in particolare di diagnosi, referti, immagini cliniche e informazioni genetiche. Lasciamo da parte il problema dei dati biometrici nonostante sia oggetto di grande attenzione da parte del regolamento IA nel caso in cui servano a identificare le persone (cosa che non dovrebbe riguardare l'ambito sanitario).

[93] Come è stato, in Italia, il caso dell'introduzione dell'art. 2-*sexies* del Codice della Privacy.

[94] Si v. in particolare il considerando n. 9 della Dichiarazione sui diritti e principi digitali. Sul tema, P. De Pasquale, *Sostenibilità e trasformazione digitale: paradigmi a confronto nella disciplina dell'Unione europea*, in *DUE*, n. 1, 2022, p. 67 ss.

nel rispetto delle disposizioni del regolamento (UE) 2016/679, cioè dei principi della liceità e dell'espressa finalità del trattamento appena richiamati. Il corretto addestramento di un sistema di IA, posto che si tratti di «trattamento» ai sensi del GDPR, è una finalità di interesse generale? Questa domanda resta al momento inevasa. Con ogni probabilità, ad essa è destinato a dare risposta il legislatore nazionale, pur sempre nel rispetto del diritto dell'Unione.

In ultimo, sempre l'art. 22 del GDPR, questa volta al suo par. 3, richiede che sia assicurato «almeno l'intervento umano da parte del titolare del trattamento» in caso di una decisione basata unicamente sul trattamento automatizzato; mentre l'art. 14 del regolamento IA pone un obbligo di sorveglianza umana solo per l'uso di sistemi ad alto rischio, con conseguente sdoppiamento (o duplicazione?) dell'obbligo, per il titolare del trattamento ai sensi del GDPR e per il *deployer* di un sistema di IA.

3.3. Segue: *la coerenza con il regolamento sullo spazio europeo dei dati sanitari e con il regolamento relativo alla* governance *europea dei dati*

Infine, vi sono altri atti, almeno due, con i quali il regolamento sull'IA interagisce da vicino in ambito sanitario: il futuro regolamento sullo spazio europeo dei dati sanitari (SEDS) e il c.d. *Data Governance Act*[95].

Infatti, il buon funzionamento di un sistema di IA è strettamente correlato alla quantità e qualità di dati che gli vengono forniti e dunque, per quel che qui in particolare ci interessa, con i meccanismi del c.d. «uso secondario» dei dati. Questi due atti, sebbene abbiano ambiti di applicazione diversi, intendono entrambi favorire lo scambio dei dati in spazi e condizioni sicure, al fine di creare un incentivo per la ricerca e l'innovazione.

In ambito sanitario, l'importanza della circolazione dei dati si accompagna al problema della loro qualità. Qui, infatti, eventuali inesattezze o errori contenuti *ab origine* nei dati trattati rischiano di produrre errori di profilassi, "*bias*" e gravi effetti discriminatori sul trattamento dei pazienti[96]. Si tratta di

[95] Rispettivamente proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari (*SEDS*, infra) e regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla *governance* dei dati).

[96] Si tratta del problema della c.d. discriminazione algoritmica, su cui M. A. K., İBRAHIM, *Legal Challenges of Artificial Intelligence in Healthcare*, in M. KILIÇ, S. B. KAHYAOİLU (eds.), *Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence*, Singapore, 2023, p. 147 ss.

problemi da risolvere alla radice e, in tal senso, soccorre il regolamento sullo SEDS, il quale, ai sensi del considerando n. 43, persegue anche lo scopo di «sostenere lo sviluppo dell'IA in ambito sanitario». In base a tale regolamento è possibile rendere disponibili i dati relativi alla salute a fini diversi da quelli per i quali sono stati in principio raccolti, attraverso un meccanismo di condivisione che, data la sua rilevanza di interesse pubblico, prescinde dal consenso del titolare dei dati[97].

In particolare, l'art. 34, par. 1, di questo regolamento elenca le finalità in base alle quali gli organismi responsabili possono fornire l'accesso ai dati sanitari elettronici a fini secondari. In particolare., le lettere *f), g) e h)* menzionano «attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici»; «attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici»; l'«erogazione di un'assistenza sanitaria personalizzata che consiste nel valutare, mantenere o ripristinare lo stato di salute delle persone fisiche sulla base dei dati sanitari di altre persone fisiche».

Analogamente, il c.d. *Data Governance Act* consente il riutilizzo di categorie di dati detenuti da enti pubblici per finalità di interesse generale, come la ricerca scientifica e lo sviluppo di più efficienti politiche sanitarie. Esso si applica però solo ai c.d. «prodotti connessi» che saranno sviluppati in ambito sanitario[98] e consente all'utente che intende utilizzarli, o a un terzo indicato da quest'ultimo, di accedere ai dati ivi contenuti[99]. Inoltre, il capo IV regola il c.d. «altruismo dei dati», il quale consente il riutilizzo, senza consenso, dei dati forniti gratuitamente dall'utente per perseguire fini di interesse generale, tra i quali potrebbe, a ragione, rientrare il miglioramento della qualità delle cure e della salute delle persone[100].

In entrambi i casi, la possibilità di riutilizzo dei dati secondari dovrà

[97] Ma l'art. 33, par. 5, della proposta di regolamento SEDS prevede che il consenso può essere richiesto all'individuo sulla base del diritto nazionale qualora si tratti di fornire accesso ai suoi dati sanitari elettronici.

[98] Considerando n. 14 del regolamento (UE) 2022/868, cit.

[99] *Ibidem*, artt. 4 e 5.

[100] G. Resta, *La dimensione collettiva dei dati personali*, in *Parolechiave*, 2023, p. 89 ss.

sempre rispondere al rispetto del principio di esattezza iscritto nel GDPR[101]. Ciò potrebbe comportare una riduzione *ex ante* del rischio di discriminazione, agendo direttamente sulla fase di addestramento degli algoritmi. In questa fase, come noto, la capacità del sistema di IA di effettuare predizioni corrette, relative, ad esempio, al rischio di sviluppare malattie o al decorso delle stesse, si basa sostanzialmente sul numero e sulla qualità dei dati forniti[102]. Questi ultimi sono tanto più accurati quanto più si basano su dati personali e sui c.d. *real world data experience*. Tutto ciò non può che avere un impatto benefico sul buon funzionamento dei sistemi di IA, garantendo il rispetto del regolamento.

3.4. Segue: *la coerenza con la legislazione in via di adozione*

Restano invece del tutto fuori dall'ambito di interferenza del regolamento IA una serie di atti e normative, sia da ridisegnare *ex novo*, come la proposta di direttiva sulla responsabilità per danno da prodotti difettosi in caso di danni prodotti dai sistemi di IA[103], sia da modificare, come nel caso del regolamento macchine[104] e della direttiva sulla sicurezza generale dei prodotti[105].

Lo stesso vale per le normative nazionali, destinate a integrare il regolamento IA, attraverso previsioni relative al diritto sulla responsabilità medica e al diritto penale.

In Italia, si segnala il disegno di legge in materia di «Disposizioni e delega al Governo in materia di intelligenza artificiale»[106], il quale emana norme che «si interpretano e si applicano conformemente al diritto dell'Unione Europea»[107]. Tra queste si segnalano in particolare le disposizioni relative al settore sanitario che prevedono il diritto dell'interessato ad essere informato circa l'utilizzo dei sistemi di IA; la spettanza dell'ultima decisione alla professione medica; la classificazione come «di rilevante interesse pubblico» dei

[101] Art. 5, par. 1., lett. *d)*, del GDPR.

[102] «*Data bias needs to be avoided by using appropriate algorithms based on un-biased real time data*» in N. Naik et al., *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, in *Frontiers in Surgery*, vol. 9, 2022, p. 5.

[103] www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en

[104] www.ec.europa.eu/docsroom/documents/45508.

[105] www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0346.

[106] Disegno di legge S 1146, www.senato.it/service/PDF/PDFServer/DF/437373.pdf

[107] *Ibidem*, art. 2, par. 1.

trattamenti di dati, anche personali, da, parte di soggetti pubblici e privati senza scopo di lucro, «per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di IA per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, di salute pubblica, incolumità della persona, salute e sicurezza sanitaria, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base»[108].

4. *Brevi riflessioni conclusive*

È molto difficile, allo stato attuale, fare previsioni sul successo o meno del nuovo regolamento IA. Certo è che si tratta di uno sforzo di regolazione molto complesso e strutturato, che ha indubbiamente la grande aspirazione di fare da modello per la circolazione di una IA sicura ed affidabile. Questo modello si preoccupa di coniugare un approccio "classico" alla regolazione con uno particolarmente "innovativo". Quest'ultimo, come anticipato, tenta di integrare e allargare la normativa di armonizzazione dell'Unione sulla circolazione e sicurezza dei prodotti con considerazioni nuove, "sistemiche", volte a garantire la struttura portante del diritto dell'Unione: i suoi valori e i diritti fondamentali che esso garantisce.

La sicurezza e l'affidabilità dei sistemi di IA si basano su regole di "*compliance*", le quali, se rispettate, dovrebbero anticipare la protezione dei beni giuridici che l'Unione intende garantire in maniera "sistemica", tra i quali senz'altro rientra il diritto alla salute. La realizzazione di obiettivi così diversificati e ambiziosi, però, finisce col dipendere molto dalla buona volontà degli attori coinvolti[109], da una struttura di *governance* aperta e agile, dall'adozione di ulteriori atti delegati da parte della Commissione e di norme di attuazione da parte degli Stati membri[110].

La necessaria buona volontà degli attori coinvolti si deduce, in particolare, dalla tipologia di obblighi cui sono sottoposti i fornitori e i *deployer*. Obblighi che abbiamo definito come essenzialmente "procedurali", poiché volti a comprovare la coerenza dei comportamenti con le regole, al fine di

[108] *Ibidem*, art. 8, par. 1.

[109] Sul tema, A. Simoncini, E. Cremona, *op. cit.*

[110] Il regolamento, da questo punto di vista, costituisce infatti una sorta di "direttiva mascherata".

garantire *ex ante* la sicurezza del sistema[111]. In alcuni casi, come quelli dei sistemi indipendenti, questo sforzo si concretizza però in una auto-valutazione non necessariamente obiettiva[112]. Per mitigare questo rischio, risulterà essenziale la definizione degli standard da parte di organismi come il CEN, il CENELEC e l'ETSI. Inoltre, lo stesso "*AI office*", di nuova creazione, si è già impegnato a fornire al più presto dei *templates* predefiniti al fine di certificare l'adeguatezza di tali sistemi.

Il regolamento, poi, potrebbe dar luogo a un'applicazione troppo lasca, anche a causa dell'inserimento di deroghe estremamente ampie. Ad esempio, i sistemi indipendenti, sebbene inseriti nell'Allegato III e dunque astrattamente classificabili come ad alto rischio, possono, in concreto, smarcarsi dall'applicazione degli ingenti obblighi scaturenti da tale livello di rischio, sulla base di una valutazione da essi stessi effettuata e non necessariamente sottoposta a verifica da parte di un organismo pubblico, in virtù dele deroghe inscritte nel par. 3 dell'art. 6 del regolamento.

Al momento mancano, in quest'ottica «proceduralizzante» ispirata al GDPR[113], adeguati controlli *ex post* sull'adeguatezza dei sistemi che abbiano già ottenuto l'immissione nel mercato. Inoltre, l'idea di disciplinare *ex ante* la sicurezza di tali sistemi, al fine di prevenire *in nuce* la realizzazione di un rischio, mal si sposa con una applicazione del principio di precauzione, in particolare in materia sanitaria.

Infine, sempre nell'ottica "proceduralizzante" prescelta, lo spazio dedicato dal regolamento alla tutela della persona appare esiguo. Infatti, quest'ultima non figura come "beneficiario delle prestazioni" o come "destinatario delle decisioni algoritmiche" nel regolamento IA, neppure in presenza di una figura particolarmente vulnerabile come quella del paziente[114].

[111] Si tratta dunque di obblighi di "*compliance*", e per questo da noi definiti come essenzialmente procedurali. Si v. sul tema, G. Gentile, *The (In)Effectiveness of EU Data Protection: A Rejoinder*, in I. Spiecker, L. Schertel Ferreira Mendes, R. Campos (eds.), *Digital Constitutionalism,* Baden-Baden, *forthcoming*.

[112] Tanto che in sede di parere il Comitato economico e sociale aveva suggerito di introdurre una valutazione della conformità da parte di un organo terzo per tutti i sistemi ad alto rischio.

[114] H. Van Kolfschooten, *EU regulation of artificial intelligence: Challenges for patients' rights*, in *CMLR*, n. 1, 2022, p. 81 ss.

In quest'ultimo caso, la tutela della vita del paziente appare particolarmente complessa dacché, come noto, il diritto alle cure è un diritto "individuale" e "sociale", condizionato dalle capacità dello Stato di offrire un adeguato servizio sanitario. Quest'ultimo dovrà quindi necessariamente confrontarsi con lo sviluppo dei sistemi di IA da utilizzare nella rete del servizio sanitario, conformandosi al regolamento, ma al contempo definendo e implementando quegli obiettivi di interesse generale di cui rimane il principale garante.

Abstract (ita)

In questo scritto ci occupiamo di analizzare l'applicazione del regolamento sull'intelligenza artificiale dell'Unione europea all'ambito sanitario e della tutela della salute, considerati uno dei c.d. "settori ad alto impatto" che maggiormente saranno riguardati da tale nuova disciplina. Per questo, particolare attenzione è dedicata allo studio della classificazione dei sistemi c.d. "ad alto rischio" e degli obblighi gravanti sugli operatori. Successivamente è analizzata la coerenza di questo nuovo quadro regolatorio con le norme già in vigore, che disciplinano ambiti affini o che comunque a questo rischiano di sovrapporsi per oggetto o per scopo. In ultimo, tentiamo di ragionare sulle modalità e sull'efficacia dell'approccio regolatorio prescelto al fine di assicurare la tutela del diritto alla salute, in ossequio ai fini dichiarati dal legislatore stesso.

Abstract (eng)

In this paper, we analyze the application of the EU Artificial Intelligence Regulation in the field of health and health protection, considered one of the so-called "high-impact sectors" that will be most affected by this new discipline. For this reason, particular attention is dedicated to the study of the classification of so-called "high-risk" systems and the obligations on these burdens, as this class will include most of the AI systems to be used in the sector of our concern. Subsequently, we investigate the consistency of this new regulatory framework with the rules already in force, which regulate similar areas, or which can overlap with the AI Act by object or purpose. Still, a general framing is dedicated to the legislations of future entry into force. Finally, we try to think about the methods and effectiveness of the regulatory approach chosen and its capability to ensure the protection of the right to health, in accordance with the purposes declared by the EU legislator itself.

IL RUOLO DELL'INTELLIGENZA ARTIFICIALE NEL PARADIGMA EUROPEO DELL'*E-JUSTICE* PRIME RIFLESSIONI ALLA LUCE DELL'*AI ACT*

Angela Correra*

SOMMARIO: 1. Considerazioni generali. – 2. Il paradigma europeo dell'*E-justice*. – 3. I vantaggi dell'impiego dell'IA nel settore della giustizia. – 3.1. Gli svantaggi dell'impiego dell'IA nella giustizia. – 4. La Corte di giustizia traccia la rotta per un'IA etica e trasparente nel settore giudiziario. – 5. Il regolamento europeo sull'IA e le sue implicazioni per il settore giudiziario. – 5.1. *Segue*: la *governance* dei dati e il dovere di trasparenza. – 6. Riflessioni conclusive.

1. *Considerazioni generali*

La pervasività delle tecnologie più avanzate come quelle che si basano su strumenti di Intelligenza artificiale (IA) ha determinato l'ingresso di sistemi computazionali nei più disparati contesti del vivere quotidiano. Ormai comunemente impiegata in numerosi settori, l'utilizzo dell'IA si sta progressivamente affermando anche nel campo della giustizia, offrendo la possibilità di ottimizzare le attività e incrementare l'efficienza dell'intero settore, ma, al contempo, manifestando caratteristiche suscettibili di condizionare pesantemente i processi decisionali, trasformandone le logiche di fondo, con importanti implicazioni sui diritti fondamentali e, più propriamente, sullo sviluppo umano.

Invero, i nuovi canali digitali e gli spazi di comunicazione generati dall'*Innovation Technology*, grazie alla crescente disponibilità dei dati, hanno dato vita ad un ecosistema digitale che ha influenzato profondamente il modo in cui gli attori del sistema giudiziario interagiscono tra loro e con coloro che chiedono giustizia[1]. I servizi legali e quelli più ampiamente attinenti all'amministrazione della giustizia, sono ormai spesso disponibili *online*, ma, dinanzi alla sfida fondamentale posta dall'IA, il sistema giudiziario dovrà compiere uno sforzo di adeguamento ulteriore, necessario se si considera che

* Assegnista di ricerca di Diritto dell'Unione europea, Università *Magna Graecia* di Catanzaro.

[1] V. G. TESAURO, *Manuale di diritto dell'Unione europea*, P. DE PASQUALE, F. FERRARO (a cura di), vol. II, Napoli, 2021, p. 331.

la concreta possibilità per gli Stati membri dell'UE di garantire un accesso alla giustizia che sia moderno, efficiente, non invasivo e senza barriere, è un indice dimostrativo del rispetto dello Stato di diritto e della democrazia, che rafforza la fiducia nel sistema istituzionale complessivamente considerato.

Appare evidente che, al cospetto di una trasformazione che investe la socialità contemporanea, la nuova stagione di dibattito tra attori pubblici e privati, in merito alle principali questioni etiche, giuridiche e sociali sull'impiego e sulle conseguenze relative all'uso di tali tecnologie[2], debba confrontarsi con il problema di sussumere entro categorie concepite prima dello sviluppo della società algoritmica fenomeni che si discostano profondamente dai paradigmi consolidati.

In proposito, la rivoluzione tecnologica ha generato nuovi interrogativi e ha aperto la strada ad ambiti di riflessione sino a qualche anno fa neanche lontanamente immaginabili, come l'impiego di algoritmi intelligenti nei processi decisionali, che, in mancanza di un puntuale intervento istituzionale, che ne orienti lo sviluppo in senso antropocentrico, rischia di determinare una situazione di sudditanza tecnologica[3], in cui l'uomo potrebbe essere relegato in una posizione di subordine rispetto alla tecnologia. Le maggiori preoccupazioni, sul punto, derivano dalla scarsa prevedibilità degli esiti di utilizzo dei sistemi di IA e dall'impatto che essa produce rispetto alla tutela dei diritti umani[4].

Per tale ragione, sul versante dell'Unione europea è stata fortemente sentita l'esigenza di una *governance* capace di garantire che le nuove tecnologie restino una forza benefica per la collettività, nella consapevolezza che i nuovi fenomeni impongono, non un mero aggiornamento, ma una profonda rivisitazione di istituti e categorie tradizionali, finora considerati come immutabili, soprattutto in contesti caratterizzati da elevata sensibilità, come quello della giustizia, ove i presidi garantistici del giusto processo, baluardo della giurisprudenza della Corte EDU e della Corte di giustizia, sembrano creare le più significative frizioni[5].

[2] V. M. Bassini, O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?* in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Milano, 2018.

[3] In tal senso, v. *Statuto etico e giuridico dell'IA*, Fondazione Leonardo, Civiltà delle macchine, p. 4, pubblicato nel mese di novembre 2019.

[4] V. diffusamente C. Grieco, *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023.

[5] Per una ricognizione dell'ampio dibattito sviluppatosi sull'impego dell'IA nel settore della giustizia, tra i molti contributi, v. F. Donati, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, n. 1, 2020; C. Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi,* in *DPCE online*, n. 3, 2020, p. 3371; Id. *Per una intelligenza artificiale costituzionalmente orientata*, in AA.VV., *Scritti per Roberto*

L'obiettivo del presente contributo è quello di esaminare l'impatto del recente regolamento n. 2024/1689[6] sull'IA sul settore dell'amministrazione della giustizia, per provare a disegnare un quadro delle prospettive future di sviluppo delle più avanzate tecnologie in tale ambito[7]. Un campo quest'ultimo tradizionalmente caratterizzato da un approccio meticoloso e spesso conservatore, ma nel quale la rivoluzione tecnologica è già molto evidente, come dimostra la crescente sensibilità manifestata dall'Unione, con l'adozione di un pacchetto di strumenti per modernizzare la giustizia in Europa[8] e la più recente strategia sull'IA della Corte di giustizia[9].

2. *Il paradigma europeo dell'*E-justice

Prima di analizzare la portata normativa e le implicazioni del regolamento, sembra opportuno svolgere alcune considerazioni di carattere preliminare sul paradigma europeo dell'*E-justice*.

Toniatti. "Pluralismo nel diritto costituzionale comparato", 2020, p. 9; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano, 2020; R. SUSSKIND, *Tribunali online e il futuro della giustizia*, Oxford, 2019; A. CARLEO (a cura di), *Decisione robotica,* Bologna, 2019; J. NIEVA FENOLL, *Intelligenza artificiale e processo*, Torino, 2019; C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi,* in *Questione Giustizia*, n. 4, 2018, p. 153; QUATTROCOLO S., U. PAGALLO, *The impact of AI on criminal law, and its twofold aspects*, in W. BARFIELD, U. PAGALLO (eds.), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham, 2018; D. BEN-ARI, Y. FRISH, A. LAZOVSKI, U. ELDAN, D. GREENBAUM, *Artificial intelligence in the Practice of Law: An analysis and proof of concept experiment*, in *Richmond Journal of Law and Technology*, 2017, p. 7.

[6] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

[7] Tra gli altri contributi sul tema, v. G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, n. 2, 2024; e, prima dell'approvazione dell'*AI Act*, M. FASAN, *L'intelligenza artificiale nel settore della giustizia. Prime riflessioni alla luce della proposta di Regolamento (UE) in materia di AI*, in *Queste Istituzioni*, n. 4, 2022, pp. 190-211.

[8] COM (2020) 710 final, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Digitalizzazione della giustizia nell'Unione europea. Un pacchetto di opportunità*, 2 dicembre 2020, su cui v. A. CIPRANDI, *La Commissione e le nuove sfide nell'era digitale: un pacchetto di strumenti per modernizzare i sistemi giudiziari nell'Unione europea*, in *EJ*, 4 gennaio 2021.

[9] V. Corte di giustizia, *Artificial Intelligence Strategy*, disponibile al seguente link: https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-11/cjeu_ai_strategy.pdf

Il contesto storico dell'impiego di strumenti informatici nell'amministrazione della giustizia nell'Unione europea è profondo e complesso, con radici che affondano nella necessità di modernizzare e rendere più efficienti le procedure giudiziarie.

La stessa Corte di giustizia, evidentemente inseguendo l'aspirazione di diventare una "smart court", ha iniziato a esplorare le possibilità offerte dagli algoritmi di IA da diversi anni. Con questo spirito, nel 2019, è stato creato l'*Innovation Lab*, con l'obiettivo di studiare le tecnologie emergenti e il modo in cui la Corte può sfruttarle; e, appena un anno dopo, è stato costituito l'*AI+ Network*, che riunisce un membro rappresentativo di ogni dipartimento, delle due cancellerie e delle sezioni della Corte e del Tribunale UE, grazie al quale sono state intraprese diverse iniziative per la digitalizzazione della giustizia nell'Unione.

Tra queste, una tappa molto importante è stata, ad esempio, la creazione del sistema integrato di gestione delle cause (SIGA) della CGUE, che sta progressivamente sostituendo un ampio numero di applicazioni attualmente in uso, offrendo la possibilità di una maggiore ottimizzazione e automazione delle fasi processuali. Significativi sono, inoltre, lo sviluppo di nuovi motori di ricerca e l'inserimento di nuovi dati nel sito *web EUR-Lex*, che hanno agevolato l'accesso a nuovi atti normativi (in particolare, alle misure nazionali di recepimento delle direttive) e alla giurisprudenza; e, ancora, l'introduzione della firma elettronica, utilizzata per sottoscrivere le sentenze e le ordinanze del Tribunale.

In uno scenario già di per sé di grande fermento, la pandemia da Covid-19 e l'emergenza sanitaria che ad essa è seguita hanno agito come elemento di straordinaria accelerazione dei cambiamenti in corso[10]. Spinta

[10] Nel contesto del mandato d'arresto europeo, ad esempio, sebbene nessuno Stato membro avesse ufficialmente disposto misure di sospensione dei provvedimenti di esecuzione delle consegne dei soggetti interessati, le restrizioni ai viaggi, imposte per contenere la diffusione del virus, hanno creato serie difficoltà nel trasferimento della persona ricercata nello Stato di emissione del mandato. Per un'analisi di tutte le criticità che i sistemi giudiziari nazionali hanno dovuto affrontare durante la crisi della COVID-19 e delle misure di risposta europea e nazionale, v. COM/2020/710 final, cit. In particolare, la Commissione, nel richiamare espressamente le iniziative del Parlamento e del Consiglio europeo, che hanno riconosciuto il ruolo centrale della digitalizzazione, anche nel contesto della giustizia, in seguito alla pandemia (risoluzione del Parlamento europeo, del 17 aprile 2020, in tema di contrasto alla pandemia da Covid-19; il documento del Consiglio europeo *Una tabella di marcia per la ripresa – Verso un'Europa più resiliente, sostenibile ed equa*, approvato il 23 aprile 2020 e le conclusioni del Consiglio *Accesso alla giustizia – Cogliere l'opportunità della digitalizzazione* già menzionate, nelle quali vengono elaborate specifiche proposte per il rafforzamento delle

dall'esigenza di limitare il più possibile la circolazione delle persone, la Corte di giustizia si è avvalsa delle moderne tecnologie per digitalizzare alcuni processi o, ancora, della tecnica della videoconferenza per svolgere le udienze a distanza. Ed è apparso subito chiaro come l'istituzione di un sistema di *streaming* per le udienze della Corte sia servito a creare condizioni di maggiore accessibilità per il grande pubblico.

Importanti passi in avanti, da un punto di vista tecnologico, sono stati poi scanditi da puntuali interventi normativi, come l'emanazione del regolamento relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema *e-CODEX*)[11], che ha offerto un quadro adeguato per lo scambio di informazioni giudiziarie attraverso servizi sicuri; dei regolamenti sulla notificazione o comunicazione degli atti[12] e sull'assunzione delle prove[13], che istituiscono l'uso del sistema informatico decentrato con punti di accesso interoperabili basati su *e-CODEX* per le comunicazioni pertinenti; del regolamento sulle prove elettroniche[14] e, in particolare, del regolamento e della direttiva sulla digitalizzazione della cooperazione giudiziaria transfrontaliera e dell'accesso alla giustizia (il cd. «pacchetto sulla digitalizzazione»)[15].

politiche relative all'accesso effettivo alla giustizia e alla digitalizzazione), proprio al fine di aumentare la resilienza dei sistemi giudiziari, nonché di migliorare l'accesso alla giustizia da parte di cittadini e imprese, incoraggia ampiamente il ricorso alle applicazioni di intelligenza artificiale, mettendo in luce i numerosi vantaggi connessi al loro utilizzo (v. punto 3.3).

[11] Regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726.

[12] Regolamento (UE) 2020/1784 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativo alla notificazione e alla comunicazione negli Stati membri degli atti giudiziari ed extragiudiziali in materia civile o commerciale ("notificazione o comunicazione degli atti") (rifusione).

[13] Regolamento (UE) 2020/1783 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativo alla cooperazione fra le autorità giudiziarie degli Stati membri nell'assunzione delle prove in materia civile o commerciale (assunzione delle prove) (rifusione).

[14] Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali.

[15] Regolamento (UE) 2023/2844 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, sulla digitalizzazione della cooperazione giudiziaria e dell'accesso alla giustizia in materia civile, commerciale e penale a livello transfrontaliero e che modifica taluni atti nel

Su questa scia, con diverse velocità e con specifiche peculiarità nei singoli Stati membri, il settore della giustizia è stato pervaso dall'inesorabile filtrare di strumenti computazionali che garantiscono la trattazione automatizzata di grandi quantità di dati per diverse finalità, con tempi e costi assai ridotti. L'IA ha così trovato applicazioni effettivamente sempre più diffuse nel sistema della giustizia di molti Stati membri, in specie con riferimento ai programmi di videoscrittura e alle banche dati di giurisprudenza[16], vale a dire applicazioni di quella che viene comunemente definita come IA "debole"[17].

In queste ipotesi, attraverso il ricorso ad algoritmi di IA applicati a *smart data* giuridici sono stati sviluppati sistemi in grado di soddisfare bisogni informativi che difficilmente potrebbero essere garantiti con i tradizionali motori di ricerca[18]. Allo stesso modo, esperienze concrete sono individuabili nell'ambito della mediazione privata di controversie mediante il *web*[19] e che l'Unione europea ha inteso incoraggiare con l'emanazione della direttiva

settore della cooperazione giudiziaria; direttiva (UE) 2023/2843 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che modifica le direttive 2011/99/UE e 2014/41/UE del Parlamento europeo e del Consiglio, la direttiva 2003/8/CE del Consiglio e le decisioni quadro 2002/584/GAI, 2003/577/GAI, 2005/214/GAI, 2006/783/GAI, 2008/909/GAI, 2008/947/GAI, 2009/829/GAI e 2009/948/GAI del Consiglio, per quanto riguarda la digitalizzazione della cooperazione giudiziaria.

[16] Molti strumenti sono considerati particolarmente promettenti, tanto che taluni ritengono che i tribunali online saranno la principale modalità di risoluzione delle controversie entro il 2030, A. Kaplan, *Online courts, the future of justice and being bold in 2020*, in *Abajournal*, 2020. Per i dettagli vedere, ad esempio, CEPEJ, Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e nel loro ambiente, 2018, p. 17.

[17] Cfr. D. Ben-Ari, Y. Frish, A. Lazovski, U. Eldan, D. Greenbaum, *Artificial intelligence in the Practice of Law: An analysis and proof of concept experiment*, in *23 Richmond Journal of Law and Technology*, 2017, p. 7.

[18] In proposito, la banca dati sviluppata presso l'Ufficio delle pubblicazioni dell'Unione europea raccoglie tutti i documenti realizzati dalle Istituzioni europee e allo stato costituisce la principale fonte di *Eur-Lex*, attraverso la quale è possibile accedere a diverse risorse giuridiche (trattati, legislazione, proposte legislative della Commissione, del Consiglio e del Parlamento UE e sentenze della Corte della giustizia). Cfr. E. Francesconi, M. W. Küster, P. Gratz, S. Thelen, *The Ontology-Based Approach of the Publications Office of the EU for Document Accessibility and Open Data Services*, in A. Kİ, E. Francesconi (eds.), *Electronic Government and the Information Systems Perspective,* Cham, 2015, pp. 29-39.

[19] Si veda, ad esempio, in "Risoluzione delle controversie online per rivendicazioni civili di basso valore", *Inghilterra e Galles: Civil Justice Council*, 2015; v. anche R. Susskind, *Tribunali online e il futuro della giustizia*, Oxford, 2019; C. Xiao et al., *CAIL2019-SCM: A Dataset of Similar Case Matching in Legal Domain*, 2019; K.D. Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*, Cambridge, 2017, p. 5.

2013/11/UE[20] e del regolamento n. 524/2013[21]. In effetti, le *Online Dispute Resolution* (ODR), nella prospettiva più moderna, sono state in alcuni casi anche istituzionalizzate e, dunque, non sono estranee alla giurisdizione, ma entrano a farne parte.

L'espansione di strumenti algoritmici è tuttavia suscettibile di numerosi altri impieghi, interessando valutazioni tecniche che vanno dalla quantificazione del danno in caso di lesioni personali, in materia civile, al calcolo della recidiva, in materia penale; all'analisi di clausole contrattuali numerose e complesse; alla selezione dei precedenti più rilevanti o dei passaggi motivazionali più rispondenti alle fattispecie in esame[22]; al sostegno della attività di indagine di polizia (c.d. *predictive policing*), sino alla possibilità di determinare l'eventuale esito di una controversia nell'ambito dell'affascinante scenario della c.d. giustizia predittiva[23].

Mentre queste ultime tecnologie sono state (solo) timidamente impiegate dalla magistratura nel panorama europeo, gli avvocati e le *law firms* del settore privato - soprattutto negli Stati Uniti e in Cina - utilizzano già strumenti di giustizia predittiva per consigliare i loro clienti quale strategia seguire (ad esempio avviare una causa in tribunale o scegliere forme alternative di risoluzione delle controversie), e il loro ruolo è destinato ad aumentare nella misura in cui saranno accessibili maggiori quantità di dati legali[24], come

[20] Direttiva 2013/11/UE del Parlamento europeo e del Consiglio, del 21 maggio 2013, sulla risoluzione alternativa delle controversie dei consumatori, che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (direttiva sull'ADR per i consumatori), in GUUE L 165/63 del 18 giugno 2013.

[21] Regolamento (UE) n. 524/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo alla risoluzione delle controversie online dei consumatori e che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (regolamento sull'ODR per i consumatori) GUUE L 165/1 del 18 giugno 2013.

[22] V. A. Pajno e a., *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Biolaw Journal – Rivista di BioDiritto*, n. 3, 2019, pp. 205-235; i numerosi contributi in A. Carleo (a cura di), *Decisione robotica,* cit.; Id. (a cura di), *Calcolabilità giuridica*, Bologna, 2017; A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal –Rivista di BioDiritto*, n. 1, 2019; A. Garapon, J. Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, 2018.

[23] Per un'analisi del concetto di giustizia predittiva, tra gli altri, E. Bassoli, *La Ciber-etica: luci e ombre della predittività algoritmizzata,* in *Liber amicorum per Pasquale Costanzo*, in *Consulta online*, 17 aprile 2020; C. Castelli, D. Piana, *Giustizia predittiva. La qualità della giustizia in due tempi,* cit., p. 153; N. Aletras et al., *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective,* in *PeerJ Computer Science*, 24 ottobre 2016.

[24] D. M. Katz, *Quantitative Legal Prediction or How I Learned to Stop Worrying and*

dimostrano alcuni esperimenti già in atto[25]. Tra quest'ultimi, si segnala uno studio condotto sulla giurisprudenza della Corte europea dei diritti dell'uomo che ha sperimentato, rispetto alla violazione del divieto di trattamenti inumani o degradanti di cui all'art. 3 CEDU, algoritmi in grado di predire in maniera fortemente attendibile il possibile esito di controversie[26].

3. *I vantaggi dell'impiego dell'IA nel settore della giustizia*

Data l'elevata accuratezza di questo tipo di strumenti, non sorprende che essi stiano raccogliendo negli Stati membri un grande interesse nella prospettiva di ottimizzare e automatizzare talune fasi della procedura giudiziaria[27].

Start Preparing for the Data-Driven Future of the Legal Services Industry, in *Emory Law Journal*, vol. 62, 2013, p. 909 ss.

[25] In Estonia, ad esempio, un progetto pilota ha creato un "giudice robot" che giudica le controversie relative a cause di modico valore, concentrandosi in particolare sulle fattispecie contrattuali. Il progetto prevede che il sistema di Intelligenza artificiale emetta una decisione in modo del tutto autonomo, basandosi esclusivamente sui documenti prodotti dalle parti, con possibilità di riesame della vicenda da parte di un giudice umano in caso di appello. Cfr. E. Niiler, *Can AI Be a Fair Judge in Court? Estonia Thinks So*, Wired, 25 marzo 2020. Analogamente, in Cina, la c.d. "*cyber-court*" ha trasferito online l'intera procedura amministrativa per la gestione dei casi (dal deposito della documentazione alla pubblicazione della sentenza). Inoltre, dall'inizio del 2019 la Corte Suprema del Popolo cinese gestisce, in via sperimentale, un programma pilota definito "mobile court", in cui un "giudice" chatbot guidato dall'IA gestisce in assoluta autonomia le procedure civili attraverso la piattaforma del social media *WeChat* del Paese. Cfr. H. Feng, Zhen/Xia, *Cina: Tre Tribunali del Cyberspazio ora online e aperti per gli affari*, 16 ottobre 2018; Y. Cui, *Intelligenza artificiale e modernizzazione giudiziaria*, Shanghai, 2020, p. 26; B. Harris, *Could an AI could an AI replace a judge in court?*, 11 July 2018.

[26] L'esperimento è stato condotto dall'University College of London attraverso un algoritmo che, prendendo in esame la giurisprudenza della Corte EDU in ben 584 casi, si è rivelato idoneo a valutare la violazione o meno di specifiche disposizioni della Convenzione EDU, raggiungendo un margine di successo fino al 79% dei casi. Per approfondimenti, v. N. Aletras et al., *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective,* in *PeerJ Computer Science*, 24 October 2016.

[27] In Francia, ad esempio, è largamente in uso, già da diversi anni, *Predictice*, il sistema che consente di semplificare la ricerca e l'analisi giuridica attraverso diversi strumenti, come l'accessibilità a tutte le decisioni giudiziarie disponibili in Francia, l'ottimizzazione della ricerca giuridica, l'analisi dei dati statistici (tasso di accettazione di una richiesta e importo del risarcimento probabile da ottenere) e l'accessibilità alle decisioni, alle basi giuridiche e ai testi giuridici menzionati nei documenti legali (serie di conclusioni, promemoria, ecc.). Per mag-

Per il vero, nell'ottica del miglioramento della cooperazione giudiziaria e del funzionamento del sistema della giustizia, si registra una generalizzata tendenza sia sul versante internazionale del Consiglio d'Europa[28], sia sul versante delle stituzioni UE a pianificare lo sviluppo e il crescente utilizzo dei sistemi di IA[29]; e rispetto ad essi è aperto il dibattito sulla sostituibilità dell'attività processuale tradizionale con quella virtuale e sulla compatibilità della stessa con i principi di difesa e del giusto processo, così come declinati dalla Corte di giustizia e dalla Corte EDU.

In questo quadro, molti ritengono che l'IA potrebbe accrescere la qualità delle decisioni giudiziarie e amministrative e che la sostituzione del giudice umano con una macchina intelligente sarebbe un'ipotesi addirittura auspicabile nella ricerca di una decisione oggettivamente esatta[30]. In altre parole, si sostiene che, se la macchina intelligente è capace di compiere operazioni matematiche tanto complesse che sarebbero precluse alla mente umana, le medesime *performance* potrebbero essere replicate anche nell'esercizio della funzione giurisdizionale. Nella stessa direzione, si afferma che il vero giudice

giori dettagli, v. Predictice, *Guide de la justice prédictive à destination des juristes et des avocats du XXIème siècle.* Allo strumento adottato in Francia, potremmo aggiungere il programma italiano TOGA, che è utilizzato come database intelligente per i pubblici ministeri e per gli avvocati; Jurimetria, un software statistico e predittivo che aiuta i professionisti del settore legale in Spagna ad analizzare i loro casi, sistematizzando ed estraendo contenuti da oltre 10 milioni di decisioni giudiziarie, provenienti da tutti i casi e ordini giurisdizionali; ancora, Casecruncher Alpha, che vanta un'accuratezza dell'86,6% delle previsioni effettuate. Si veda per ulteriori approfondimenti lo studio della Commissione europea sull'uso delle nuove tecnologie nei sistemi giudiziari.

[28] Al Consiglio d'Europa si deve l'emanazione della Carta etica europea sull'impiego dell'IA nei sistemi giudiziari e negli ambienti connessi, che stabilisce cinque principi sostanziali e metodologici che si applicano al trattamento automatizzato delle decisioni e dei dati giudiziari, basato su tecniche di IA V. Commissione europea per l'efficienza della giustizia (CEPEJ), *European Ethical Charter for the use of artificial intelligence in judicial systems and their environment*, December 2018. La Carta etica, il cui contenuto sostanziale potrebbe confluire in un atto giuridicamente vincolante, costituisce il primo tentativo verso la definizione di risposte concrete alle preoccupazioni che i sistemi algoritmici applicati alla giustizia sollevano in relazione al *fair trail* e al *due process*. Più recentemente, è stata approvata la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto, aperta alla firma a partire dal 5 settembre 2024.

[29] Consiglio dell'Unione europea, *Strategia europea in materia di giustizia elettronica 2024-2028*, 15509/23, 17 novembre 2023.

[30] V. D. M. Katz, *Quantitative Legal Prediction - Or - How I Learned to Stop Worrying and Start Preparing for the Data-driven Future of the Legal Services Industry*, in *Emory Law Journal*, 2013; R.M. Re, A. Solow-Niederman, in *The Stanford Technology Law Review*, 2019, p. 246 ss., spec. p. 255.

terzo e imparziale, autonomo e indipendente, sia proprio quello artificiale che, lontano dalle pulsioni e dalle emozioni dell'animo umano, potrebbe essere assunto come il migliore interprete di quell'ambizione che ogni ordinamento giuridico si tramanda e, cioè, la certezza del diritto e l'uguaglianza dinanzi alla legge[31].

Sennonché, per quanto suggestive possano essere tali considerazioni, è necessaria una riflessione in chiave problematica di fenomeni in rapida evoluzione che potrebbero sì determinare un deciso miglioramento dei tempi della giustizia, ma che nascondono anche molte insidie. A tal fine, è opportuno distinguere gli impieghi dell'IA che andrebbero incoraggiati da quelli che dovrebbero essere vincolati a talune restrizioni.

Anzitutto, basti pensare alle operazioni generalmente connesse all'esercizio della *potestas iudicandi* - come la sussunzione della fattispecie concreta in quella astratta, la valutazione dei fatti rilevanti, la individuazione della fonte normativa nazionale o sovranazionale applicabile al caso concreto o la risoluzione delle antinomie - per convincersi che esse non si risolvono nella mera elaborazione di un sillogismo automatico, ma implicano un'attività creativa di confronto e di intuizioni, che difficilmente potrebbe essere rimessa (almeno non in via esclusiva) ad una applicazione meccanica di giustizia predittiva[32].

Alla luce di tali considerazioni, le valutazioni delle Istituzioni UE si stanno concentrando sull'impiego degli strumenti di IA in funzione tutoria dell'attività giurisdizionale.

In tale ottica, il Consiglio UE ha rilevato che la digitalizzazione della giustizia, grazie all'impiego delle tecniche di IA, potrebbe facilitare l'accesso alla giustizia per i cittadini in tutta l'UE, contribuire a strutturare meglio i procedimenti ed accelerare la gestione di compiti standardizzati e uniformi[33]. Sulla stessa scia, la Commissione UE ha sottolineato l'importanza dell'interoperabilità dei dati e di opportune sinergie in direzione del miglioramento della cooperazione giudiziaria tra gli Stati membri dell'Unione[34]. E, da ultimo, la Corte di giustizia ha elaborato una propria strategia sull'IA

[31] In tal senso, v. E. Vincenti, *Il "problema" del giudice-robot*, in A. Carleo, *Decisione robotica,* cit., p. 111.

[32] Cfr. M. Luciani, *La decisione giudiziaria robotica*, *ibidem*; ma anche C. Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE online*, n. 3, 2020, pp. 3369-3389.

[33] Conclusioni del Consiglio «*Accesso alla giustizia - Cogliere le opportunità della digitalizzazione*», 2020/C 342 I/01 GU C 342I del 14 ottobre 2020, pp. 1–7.

[34] Commissione europea, *Study on the use of innovative technologies in the justice field – Final Report,* September 2020.

evidenziandone le straordinarie potenzialità nella riduzione della durata del giudizio e del margine di errore nelle cause, in una epoca in cui la diversità e la lentezza nelle decisioni dei giudici sono percepite come un fattore patologico della funzione giurisdizionale[35].

3.1. *Gli svantaggi dell'impiego dell'IA nella giustizia*

Nondimeno, ad onta degli indiscutibili vantaggi, in termini di semplificazione e di accelerazione, derivanti dall'automazione di specifiche operazioni propedeutiche e strumentali alla fase di "giudizio", il ricorso a modelli decisionali automatizzati comporta sfide inedite per il rispetto dei principi fondamentali del processo, sui quali si fonda la disciplina dell'Unione; per cui, un atteggiamento realistico ha indotto le Istituzioni UE alla segnalazione dei rischi connessi all'impiego delle nuove tecnologie e degli strumenti di IA nel settore della giustizia, in specie per quel che concerne il momento decisionale.

Il riferimento è anzitutto alle significative implicazioni che gli strumenti di natura predittiva sono suscettibili di produrre sui presidi previsti a garanzia di un processo equo, in termini di processi decisionali opachi, di conseguenze pregiudizievoli sull'imparzialità e sull'indipendenza del giudice, sulla parità delle armi, sul contradditorio e sul diritto ad un ricorso effettivo a fronte di una decisione anche solo parzialmente automatizzata, con l'emersione delle maggiori criticità soprattutto con riferimento alla disciplina in materia penale[36]. In particolare, nella prospettiva del giusto processo, del rispetto del diritto di difesa e del diritto ad un ricorso effettivo di cui all'art. 47 della Carta dei diritti fondamentali dell'Unione, esiste un rapporto di tensione tra i modelli decisionali automatizzati e l'impostazione tradizionale che generalmente affida i valori in gioco ad una decisione umana, accessibile e controllata.

Nello specifico, tra i rischi connessi alla diffusione dell'IA nel settore

[35] La risoluzione dell'endemico problema della lentezza della giustizia, non a caso, è stata posta dalla Commissione UE come condizione per l'assegnazione dei fondi di Next Generation UE sulla base dell'osservazione che una giustizia lenta equivale ad una giustizia denegata e ha un'influenza negativa sullo sviluppo economico e sulle capacità democratiche di un Paese.

[36] Sulle principali questioni connesse all'applicazione dell'intelligenza artificiale nei procedimenti penali da una prospettiva europea si veda S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Cham, 2020.

della giustizia, nella narrativa delle Istituzioni UE sembrano sollevare le maggiori preoccupazioni quelli legati alla divulgazione di dati sensibili, alla potenziale introduzione di distorsioni durante l'addestramento dei modelli di IA, nonché alla generazione di informazioni false.

A ciò si aggiungono i problemi di scarsa trasparenza o opacità del processo decisionale, importantissimi in ambito giurisdizionale, riconducibili al fenomeno della *black box*, che di fatto non consentono di comprendere i passaggi logici attraverso i quali l'IA sia pervenuta ad una data previsione o decisione[37].

Da una parte, l'impossibilità di accedere alle informazioni necessarie su cui si basano i modelli decisionali più avanzati fondati sull'IA, può tradursi in un vizio motivazionale delle sentenze emanate anche con il semplice supporto di queste tecnologie, generando un contesto di asimmetria informativa incompatibile con il rispetto del diritto di difesa e della parità delle armi. Dall'altra parte, il fenomeno della *black box* può determinare un problema di compatibilità con i requisiti di imparzialità e terzietà del giudice con gli ambiti di discrezionalità della decisione che l'esercizio della funzione giurisdizionale normalmente implica.

Più specificamente, i sistemi di *open access*, come quelli sopra ricordati, unitamente agli strumenti di natura predittiva, potrebbero avere un significativo impatto sul piano della portata del precedente giurisprudenziale e dell'indipendenza dell'organo giudicante[38]. Sebbene l'accesso completo alle raccolte giurisprudenziali garantisca una migliore circolazione delle sentenze e agevoli l'attività dei professionisti legali, consentendo di prevedere come un giudice potrà valutare una data controversia o come deciderà nell'ambito del collegio nel quale siede, va, tuttavia, segnalato che potrebbero verificarsi anche serie criticità.

Alcuni studi dimostrano, ad esempio, che dal *set* di dati utilizzati per addestrare l'IA potrebbero derivare *bias* o pregiudizi[39], che inavvertitamente

[37] Cfr., per tutti, F. Pasquale, *The Black Box Society*, Harvard, 2016.

[38] Cfr. A. Pajno e a., *op. cit.* p. 229.

[39] Uno studio del 2016 di ProPublica ha scoperto che COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) - un sistema algoritmico di predizione del rischio di recidivanza e di comportamenti violenti di proprietà di una società privata, ampiamente impiegato in alcune corti americane - avrebbe assegnato agli afroamericani un tasso di recidiva ad alto rischio doppio rispetto alle altre popolazioni, mentre gli imputati bianchi venivano erroneamente etichettati a basso rischio più spesso delle persone di colore. Cfr. J.Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks,* ProPublica, 2016; B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *The Ethics of Algorithms:*

riflettono o amplificano gli stereotipi esistenti o le precomprensioni di chi elabora l'algoritmo e la cui ideologia potrebbe influenzare il comportamento della macchina, portando a interpretazioni distorte o false dichiarazioni[40].

Inoltre, come ben evidenzia la Corte di giustizia nella sua recente strategia sull'IA, un eccessivo affidamento sulla tecnologia senza l'apporto di un pensiero umano critico potrebbe condizionare l'organo giudicante sino ad orientarne le scelte in direzione di quelle formulate dalla macchina e influenzarne inevitabilmente la motivazione[41].

La preoccupazione, diffusamente espressa anche in dottrina, è, in altre parole, che il giudice possa essere indotto ad appiattirsi sui risultati della macchina - fondati sul mero dato statistico che la maggioranza dei suoi colleghi ha deciso in una data maniera -[42] e che possa finire con l'abdicare al proprio dovere di decidere, confidando esclusivamente sull'efficacia e sulla correttezza dell'algoritmo[43], secondo quello che studiosi francesi hanno qualificato come «*effet moutonnier*»[44].

Mapping the Debate, 21 dicembre 2016. Sulla vicenda è intervenuta la Corte suprema del Winsconsin, nel caso *State/Loomis*, originato dal ricorso di un imputato avverso una decisione con cui nella determinazione del quantum della pena comminata, il giudice di primo grado aveva tenuto in considerazione "anche" il risultato fornito dal software COMPAS, il cui funzionamento per ragioni proprietarie non era stato, però, reso accessibile alla difesa. Sulla vicenda processuale, v. C. McKay, *Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decision-making,* The University of Sydney Law School, November 2019.

[40] Per identificare e mitigare questi pregiudizi è necessario mettere in atto strumenti di vigilanza costante e misure proattive, come set di dati di formazione diversificati e completi, nonché il monitoraggio e l'aggiornamento continui dei sistemi di IA per garantire equità e obiettività. Sul tema, v. A. Adinolfi, *Processi decisionali automatizzati e diritto antidiscriminatorio dell'Unione europea*, in A. Adinolfi, A. Simoncini (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022, p. 31 ss.

[41] In tal senso, in dottrina, v. anche F. Donati, *op. cit.;* A. Simoncini*, op. cit.*, p. 81.

[42] Cfr. A. Traversi, *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice* robot*?* in *Questione giustizia*, 10 aprile 2019, il quale afferma che «il sistema, potrebbe ridursi ad una gestione automatizzata di affermazioni cristallizzate» e che «la predizione non abbia più un valore "indicativo", ma quasi "prescrittivo", facendo sì che il giudice tenda ad applicare la soluzione proposta dalla macchina senza esaminarla alla luce della particolarità del caso concreto».

[43] Per approfondimenti sulla questione, v. anche C. Barbaro, *Uso dell'intelligenza artificiale nei sistemi giudiziari: verso la definizione di principi etici condivisi a livello europeo?,* in *Questione giustizia*, n. 4, 2018, p. 194.

[44] La teoria dell'«effetto gregge» che deriverebbe dalla giustizia predittiva è stata elaborata da A. Garapon, J. Lassègue, *op. cit.,* p. 239.

In tal modo, sulla base di un approccio meramente fideistico e incurante delle specificità della fattispecie concreta, la soluzione proposta dall'IA perderebbe la sua connotazione orientativa, per assumere una portata normativa, deresponsabilizzando il giudice rispetto al provvedimento che va assumendo e compromettendo significativamente l'evoluzione giurisprudenziale[45].

Di conseguenza, viene da chiedersi, nel caso in cui siffatti strumenti dovessero essere impiegati come ausilio da parte di un organo giudicante, come potrebbe conciliarsi il requisito dell'indipendenza del giudice rispetto a soluzioni automatizzate, in cui la decisione è assunta sulla base di dati e di precedenti giurisprudenziali che siano stati ritenuti rilevanti *aliunde* (per effetto dell'inserimento delle informazioni da parte del programmatore del sistema) e, quindi, pur sempre frutto di una selezione umana.

Infine, non meno rilevanti sono le note problematiche connesse al *digital divide* derivanti dalla mancanza di adeguate conoscenze in capo ai giudici o agli assistenti giudiziari.

4. *La Corte di giustizia traccia la rotta per un'IA etica e trasparente nel settore giudiziario*

Queste perplessità hanno indotto le Istituzioni europee ad assumere un atteggiamento di prudenza nell'utilizzo dell'AI e degli algoritmi nel sistema della giustizia. Nella consapevolezza che sarebbe irragionevole e antistorico rinunciare alle opportunità che essi offrono, in specie se impiegati come ausilio e riscontro rispetto alla decisione giudiziaria, esse stanno concentrando i loro sforzi nell'indagare le condizioni alle quali è possibile riconoscere i vantaggi dell'IA, dominandone gli effetti distorsivi e farne prevalere le potenzialità in positivo[46].

In questo scenario, la Corte di giustizia, nota per il suo approccio cauto nei confronti dell'innovazione tecnologica, ha più recentemente compiuto un passo significativo sviluppando una propria strategia sull'IA. Nel documento da essa prodotto viene accordato un certo favor all'adozione di nuove tecnologie, aprendo le porte ad un processo di ripensamento quasi radicale

[45] Cfr. S. Gaboriau, *Libertà e umanità del giudice: due valori fondamentali della giustizia. La giustizia digitale può garantire nel tempo la fedeltà di questi valori?,* in *Questione giustizia*, n. 4, 2018, p. 209, il quale parla di una vera e propria «dittatura del precedente».

[46] V. Consiglio UE, *A digital future for Europe*, 8 dicembre 2022 (ultimo aggiornamento), in www.consilium.europa.eu/en/ policies/a-digital-future-for-europe/.

del modo di concepire l'organizzazione della giustizia e dei processi che la governano. Su questa base, esso afferma che l'IA potrebbe svolgere un ruolo di supporto nel condurre una molteplicità di attività connesse all'amministrazione della giustizia, assistendo utilmente (anche) il giudice, senza, però, giungere a sostituirlo, in termini formali o sostanziali.

Entro tale area di intervento, l'orizzonte proposto è quello che, confermando il perentorio divieto di una decisione basata unicamente su trattamenti automatizzati di cui all'art. 22 del regolamento UE n. 2016/679, attribuisca all'algoritmo una funzione esclusivamente tutoria che limiti le occasioni di insuccesso della decisione giudiziale, nel quadro di un rapporto di collaborazione tra l'uomo e la macchina, nel rispetto del potere decisionale del giudice e dell'indipendenza della magistratura, quali espressione della *rule of law*.

Alla luce di tali considerazioni, la strategia della Corte promuove l'impiego dell'IA nel settore della giustizia per l'automazione di compiti semplici in ambito giuridico e amministrativo, nella ricerca e nella traduzione giuridica.

La strategia prevede, inoltre, che la futura interconnessione delle banche dati nazionali, aiutata da algoritmi di traduzione neurale, potrebbe ridurre significativamente le barriere linguistiche, risolvendo un aspetto cruciale per un organismo multilingue come la Corte di giustizia.

Un ulteriore elemento che il documento evidenzia riguarda i vantaggi che l'IA potrebbe portare nel migliorare l'accesso alla giustizia e alla trasparenza nei confronti dei cittadini dell'UE. Nel caso delle persone con disabilità, esse potrebbero beneficiare, ad esempio, di sottotitoli automatici per le udienze trasmesse in streaming e gli assistenti virtuali potrebbero aiutarle a soddisfare le loro richieste con risposte video o audio nella loro lingua. *Chatbot*, assistenti virtuali, *avatar AI* integrati nel sito *web* della Corte potrebbero anche supportare il pubblico in generale o i professionisti del settore nella ricerca di informazioni.

5. *Il regolamento europeo sull'IA e le sue implicazioni per il settore giudiziario*

Nella prospettiva di comprendere quale sarà il percorso da intraprendere per assicurare un uso dell'IA compatibile con le strutture e gli istituti tradizionali del settore della giustizia, soprattutto in termini di trasparenza, non discriminazione e tutela della *privacy*, appare fondamentale completare

l'analisi con l'esame delle disposizioni normative del regolamento in materia di IA che si applicheranno a tale ambito.

Senza dubbio, l'*AI Act* oggi rappresenta la parte più importante della strategia del mercato digitale europeo[47]. I numerosi contributi di questo fascicolo speciale[48] hanno ben evidenziato le difficoltà che hanno incontrato,

[47] L'intervento normativo, infatti, inscritto entro la cornice normativa delineata dall'art. 114 TFUE (in coerenza con la tendenza europea di ricondurre la politica del digitale entro l'alveo applicativo di tale norma, come sottolineato da G. Caggiano, *Il quadro normativo del Mercato unico digitale*, in *EJ*, Numero speciale "*Mercato unico digitale, dati personali e diritti fondamentali*", a cura di F. Rossi Dal Pozzo, 2020, pp. 13-49 e, ancora, da G. Caggiano, G. Contaldi, P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, si colloca nell'ambito del più ampio obiettivo della creazione del mercato unico digitale dell'UE, con l'abolizione degli ostacoli o barriere giuridiche che potrebbero compromettere l'espansione della dimensione UE in questo importante settore del mercato. Sul punto, si rimanda al contributo di M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno*, in questo *Fascicolo speciale*, soprattutto pp. 12-13. Puntuali rilievi erano già stati svolti da A. Adinolfi, *L'Unione europea dinanzi allo sviluppo dell'Intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. Dorigo (a cura di) *Il ragionamento giuridico nell'era dell'Intelligenza artificiale*, Pisa, 2020, p. 27; Id., *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in AA. VV., *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, p. 127 ss.; C. Schepisi, *Diritti fondamentali, principi democratici, e* rule of law: *quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in *Studi sull'integrazione europea*, 2022, pp. 41-69; G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, 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, Milano, 2022, pp. 222-223.

[48] V. F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in questo *Fascicolo speciale*. Con riferimento a specifiche questioni, *ivi*, v. anche C. Burelli, *Prime considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità*; E. Cirone, *L'*AI Act *e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*; C. Grieco, *Il diritto d'autore nell'*AI Act; M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*; S. Lattanzi, *Prime riflessioni sull'applicazione del nuovo regolamento sull'intelligenza artificiale al settore sanitario*; G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'*AI Act, *con particolare riferimento alle* regulatory sandboxes; S. Villani, *Il sistema di vigilanza sull'applicazione dell'*AI Act: *ognun per sé?*; A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*.

non solo le Istituzioni[49], ma anche esperti e parti interessate[50], nel creare un quadro normativo che fosse al tempo stesso innovativo e protettivo dei diritti fondamentali[51], ma soprattutto idoneo a regolare un fenomeno dai confini incerti e sfuggenti, destinato per caratteristiche intrinseche ad espandersi e, per questo, dai caratteri continuamente mutevoli[52].

Allo stesso modo, è stato già sottolineato che in questa complessa operazione, in linea con quanto preannunciato nel Libro bianco sull'IA[53], la scelta dell'UE è stata quella di prevedere un sistema di regole suscettibile di applicazione orizzontale che disciplina *in nuce* le moderne tecnologie[54].

Difatti, nel regolamento non si rinvengono regole specificamente rivolte al settore dell'amministrazione della giustizia, di interesse in questa sede, o ad altri settori. Il nuovo quadro normativo si limita a prevedere norme di carattere generale, frutto della convergenza tra competenze tecniche[55] e

[49] Per un'analisi, ad esempio, del ruolo svolto dal Parlamento europeo, v. G. DI FEDERICO, *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. DI FEDERICO (a cura di), *Alla (ri)scoperta del Parlamento europeo: 1979-2019*, Torino, 2021, pp. 71-88.

[50] Si ricordano, in proposito, le Linee guida per un'IA affidabile, elaborate dall'*High-Level Expert Group on Artificial Intelligence* istituito presso la Commissione UE (il testo delle linee guida è disponibile al seguente link https://op.europa.eu/it/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1)

[51] V. soprattutto il contributo di E. CIRONE, *L'*AI Act *e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, cit.; ma anche M. CARTA, *Il Regolamento UE sull'Intelligenza artificiale: alcune questioni aperte*, in *EJ*, n. 3, 2024, p. 189.

[52] Per un'analisi dell'approccio delle Istituzioni UE alla regolazione dell'IA prima dell'adozione dell'*AI Act*, v. C. SCHEPISI, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, pp. 53-75

[53] V. COM (2020) 65 final, *Il Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* (il testo del libro bianco è disponibile al seguente link https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approachexcellence-and-trust_de), 19 febbraio 2020, nel quale sono confluite una strategia per l'IA (COM (2018) 237 final, *L'intelligenza artificiale per l'Europa*, 25 aprile 2018) e un piano coordinato per l'allineamento delle strategie concordato con gli Stati membri.

[54] Il regolamento UE sull'IA costituisce di fatto il primo intervento normativo al mondo, di carattere sistemico e generale rivolto all'intero ecosistema relativo all'IA, dalla sua immissione sul mercato, al suo uso, nonché alle responsabilità che da tali usi potrebbero sorgere.

[55] Nella realizzazione del mercato interno, il legislatore europeo ha sovente fatto ricorso a norme tecniche di provenienza privata per definire o integrare atti vincolanti dell'UE. Per un approfondimento sull'impiego di norme armonizzate nel contesto del nuovo regolamento sull'IA, si rinvia al contributo di A. VOLPATO, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, cit.

giuridiche, che dovranno essere oggetto di futuri completamenti e accorgimenti[56]. L'obiettivo perseguito è, infatti, quello di disegnare la strada per lo sviluppo dell'IA nel mercato europeo, attraverso un'impostazione che vuole preservare la centralità dell'uomo nell'era delle macchine e riconoscere carattere di assoluta preminenza al controllo umano nei processi decisionali, suscettibili di avere profonde implicazioni sui diritti fondamentali dell'individuo.

In particolare, la logica applicata è quella di un approccio *ex ante*, fondato sui valori di cui all'art. 2 TUE, caratterizzato dalla previsione di una definizione tecnologicamente neutra di IA[57] calata in un sistema del rischio[58] potenziale[59] che cataloga gli strumenti di IA in base ad una qualificazione in termini di rischio minimo, limitato, alto[60] e inaccettabile[61]. All'individua-

[56] La necessità di adottare strumenti che consentono di adattare il quadro normativo «dinamicamente man mano che la tecnologia si evolve e emergono nuove situazioni preoccupanti» è evidenziata nella Relazione esplicativa alla proposta di regolamento, al punto 1.1. Su questo profilo, v. F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento*, cit., p. 5 ss.; ma anche C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3, 2021, pp. 419 e ss.

[57] V. art. 3 del regolamento.

[58] La scelta della graduazione delle regole sulla base dei rischi non è nuova per il legislatore europeo, visto che riflette soluzioni di *policy* già sperimentate con successo in settori affini (ad es. quello dei dispositivi medicali). Tanto è vero che lo schema proposto dal regolamento (UE) sembra ripercorrere quello già previsto nel contesto dell'Unione dalle direttive sulla etichettatura CE di alcuni prodotti, ove lo scopo delle norme tecniche e dei sistemi di certificazione è quello di consentire ai consumatori di determinare facilmente la qualità del prodotto o del servizio nei confronti del mercato; il che in linea di principio promuove la concorrenza.

[59] La matrice del rischio - strutturalmente indissociabile dagli strumenti di IA – ha ispirato l'impostazione antropocentrica su cui si fonda l'intero impianto regolatorio e colloca quest'ultimo nel contesto del *New Legislative Framework* e, cioè, l'approccio normativo alla commercializzazione UE finalizzato a garantire la circolazione di beni e servizi sicuri e il ricorso a meccanismi di controllo e monitoraggio del mercato interno.

[60] V. art. 6 del regolamento, secondo il quale «un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I».

[61] Il Capo II, all'art. 5 del regolamento, prevede tra i sistemi che determinano un rischio

zione di tali differenti classi di rischio si accompagna poi, specularmente, l'individuazione di regimi regolatori differenziati.

Nel quadro della disciplina generale sommariamente esposta, il legislatore colloca le applicazioni di IA impiegabili nel settore dell'amministrazione della giustizia tra quelle presuntivamente ritenute per caratteristiche intrinseche ad «alto rischio».

Precisamente, l'allegato III del regolamento individua un solo "caso d'uso" di applicazioni IA che possono avere un impatto sistemico sulla sicurezza degli individui e sui diritti fondamentali nel settore oggetto di analisi e, cioè, «i sistemi usati per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a un insieme concreto di fatti»[62].

In generale, in queste ipotesi, l'impego dell'IA non è vietato, ma è considerato ammissibile *sub condicione*. Più precisamente, è previsto un «sistema di gestione del rischio»[63] basato su un insieme di cautele *ex ante* ed *ex post* nella forma di valutazioni e autovalutazioni di conformità del prodotto e del rischio, di informazione e trasparenza, nonché di sicurezza e affidabilità, propedeutiche al rilascio di certificazioni obbligatorie, attraverso le quali gli operatori interessati possono dimostrare l'affidabilità dei sistemi di IA «ad alto rischio» impiegati, certificandone la conformità ai requisiti etici, giuridici e tecnici previsti nel regolamento, prima che i relativi prodotti o servizi possano essere immessi sul mercato.

Le disposizioni, se calate nella specifica dimensione giudiziaria, dovrebbero comportare che gli operatori giudiziari/utilizzatori di beni o servizi fondati su applicazioni di IA siano costantemente informati ed aggiornati circa la possibilità che essi possano condurre, ad esempio, a decisioni discriminatorie, a valutazioni deterministiche oppure ad errate cristallizzazioni della giurisprudenza, e suggerire, all'occorrenza, gli opportuni rimedi e/o correttivi[64].

inaccettabile quelli che sviluppano tecniche subliminali idonee a condizionare il comportamento altrui con probabili conseguenze fisiche o psicologiche a danno dei soggetti interessati o di altri; quelli che sfruttano le vulnerabilità di gruppi sociali fragili; quelli cd. di *social scoring*, utilizzati dalle pubbliche autorità al fine di valutare e classificare l'affidabilità delle persone fisiche sulla base del loro comportamento sociale; o, ancora, quelli che consentono l'identificazione biometrica a distanza «in tempo reale», fatta salva l'indispensabilità di esigenze pubblicistiche imperative ritenute prevalenti.

[62] V. allegato III del regolamento, punto 8, lett. a).

[63] V. art. 9 del regolamento.

[64] Su tali aspetti e criticità, v. anche C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, cit.; M. FASAN, *L'Intelligenza artificiale nel settore della giustizia*, cit.

5.1. Segue: *la* governance *dei dati e il dovere di trasparenza*

Oltre alle prescrizioni di carattere generale sopra ricordate, l'*AI Act* stabilisce regole più puntuali con riguardo alla qualità dei dati impiegati nei processi decisionali automatizzati, alla trasparenza dei meccanismi di IA e alle misure di sorveglianza umana.

Più specificamente, per l'addestramento di modelli di IA ad alto rischio, il regolamento individua determinati criteri che devono sovraintendere la realizzazione delle scelte progettuali, la raccolta e le operazioni di trattamento dei dati (in particolare, annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione), in modo tale da garantire non solo l'accessibilità, la quantità e l'adeguatezza dei *dataset* impiegati, ma anche e soprattutto per individuare, prevenire e colmare possibili distorsioni o carenze rilevanti nelle informazioni utilizzate[65].

La *ratio* di simili accorgimenti risponde, inoltre, all'esigenza di assicurare che i dati immessi nel sistema di IA durante tutto il suo ciclo vitale siano «pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista», nonché «statisticamente appropriati» per il contesto e i fini per cui il sistema verrà utilizzato.

Quest'ultimo assunto assume specifico rilievo quando oggetto di trattamento siano dati sensibili, come quelli relativi all'origine razziale o etnica, al *background* socio-economico, all'appartenenza sindacale, alle opinioni politiche, alle convinzioni religiose o filosofiche, o ancora i dati genetici, biometrici, relativi alla salute o quelli riguardanti la vita o l'orientamento sessuale di un individuo. Nel caso in cui dovesse essere identificata una discriminazione, infatti, la predisposizione di misure correttive per limitare o, se possibile, neutralizzare questi rischi e sensibilizzare le parti interessate diviene fondamentale.

Un profilo diverso, ma strettamente connesso alla disciplina dei dati impiegati, investe il rispetto del dovere di trasparenza che il regolamento impone ai fornitori e produttori di strumenti IA ad alto rischio[66]. Tale dovere si sostanzia nella necessità di progettare e sviluppare i sistemi intelligenti in modo tale che tutte le operazioni siano sufficientemente comprensibili per gli utenti finali, i quali dovranno essere in grado di interpretare i risultati dell'IA e di utilizzarla in modo appropriato.

[65] V. art. 10 del regolamento, in particolare i paragrafi da 2 a 5.

[66] V. art. 13 del regolamento.

A tale scopo, sui distributori grava l'onere di fornire «le istruzioni per l'uso del sistema», con indicazione di «informazioni chiare, concise, complete, accessibili, rilevanti e comprensibili» su ogni aspetto rilevante dell'intero ciclo di vita della macchina[67].

Nel tentativo di operare una prima proiezione dell'applicazione di tali disposizioni alle ipotesi di uso dell'IA nel contesto dell'amministrazione della giustizia, da esse deriva anzitutto la necessità che i dati impiegati provengano da fonti certificate e riportino in modo corretto le norme giuridiche applicabili al contesto di volta in volta esaminato; che offrano una ricognizione delle situazioni giuridiche rilevanti per la fattispecie considerata e un'accurata selezione degli orientamenti giurisprudenziali, assicurandosi che essi siano realmente rappresentativi dei diversi contesti fattuali in cui il giudice è chiamato a statuire e non corrispondere a schemi di analisi «preconfezionati».

In concreto, ciò dovrebbe comportare per il giudice che si avvalga degli strumenti di IA la possibilità di identificare i *bias* che potrebbero dare luogo a decisioni giudiziarie errate, ma soprattutto di accedere al set di dati immessi per comprendere le ragioni per le quali la macchina sia pervenuta ad un certo output. Un profilo quest'ultimo di cruciale importanza sia per il caso in cui il giudice voglia condividere il risultato proposto dalla macchina sia per il caso in cui voglia disattenderlo. In entrambe le ipotesi, infatti, il giudice dovrebbe essere in grado di spiegare in maniera chiara e comprensibile le ragioni per le quali abbia ritenuto di condividere il percorso «automatizzato» o di disattendere la soluzione algoritmica nella misura necessaria a consentire la contestazione della decisione.

Parimenti, la previsione dei requisiti di trasparenza dovrebbe assicurare al giudice che decida di avvalersi dell'ausilio di strumenti algoritmici tutte le informazioni necessarie sul funzionamento, sulle prestazioni e sui relativi limiti, nonché tutte le indicazioni per comprendere i risultati prodotti, in modo tale che possa impiegare tali sistemi in maniera consapevole e appropriata rispetto alle garanzie e i diritti fondamentali su cui l'attività giudiziaria che va compiendo potrebbe incidere.

Ma oltre a rendere l'operatore giudiziario maggiormente edotto circa le capacità e i limiti della macchina, gli accorgimenti in materia di trasparenza e interpretabilità dei risultati prodotti potrebbero assumere significato nel momento decisionale per agevolare il compito del giudice di motivare il provvedimento che dovesse decidere di adottare.

Completano il quadro delle cautele predisposte dal legislatore europeo

[67] V. art. 13 del regolamento, in particolare par. 3, dalla lett. a) alla lettera f).

per i sistemi di IA ad alto rischio le importantissime regole sulla sorveglianza umana e quelle sulla necessità di creare un ambiente tecnologico sicuro a garanzia dell'integrità del sistema.

Più nello specifico, il regolamento si caratterizza per l'introduzione di una sorta di «coefficiente di umanità» nel processo di funzionamento delle macchine, in forza del quale il controllo, la supervisione e il potere di intervento umano devono essere misurati in ragione della intensità e della natura dei rischi generati dall'IA e dalle tecnologie connesse[68]. In tal senso, il coinvolgimento umano può assumere la forma dell'*human-in-the-loop* (mero intervento umano), dell'*human-on-the-loop* (supervisione umana del processo) e dell'*human-in-command* (controllo umano dell'esito finale)[69].

Più specificamente, le disposizioni normative pertinenti impongono ai fornitori di progettare e sviluppare i sistemi di IA con adeguate interfacce uomo-macchina che consentano a coloro ai quali sarà affidata la supervisione umana di «comprendere correttamente le capacità e i limiti» della macchina ed essere in grado «di monitorarne debitamente il funzionamento», così da intervenire tempestivamente in caso di «anomalie, disfunzioni e prestazioni inattese».

Inoltre, all'esplicito fine di evitare il fenomeno dell'*automation bias*, le misure di sorveglianza umana impongono di informare l'utente «della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento» sull'*output* prodotto dal sistema IA, oltre che della possibilità di poter sempre disattendere, annullare o ignorare la soluzione proposta o interrompere il funzionamento della macchina ancor prima che un eventuale risultato possa essere prodotto.

Anche in questo caso, il principio *under user control* sotteso alle prescrizioni normative dovrebbe accrescere l'autonomia dell'operatore giudiziario e preservarne l'autodeterminazione durante l'impiego di strumenti di IA. In tal modo, il regolamento vuole escludere in radice un approccio prescrittivo dell'impiego dell'IA e assicurare che gli utilizzatori agiscano come soggetti informati e conservino il pieno controllo delle loro scelte.

In considerazione del fatto che l'utente può essere sia l'operatore di diritto che utilizza il tool sia il destinatario della decisione, tale principio

[68] V. art. 14 del regolamento.

[69] Sul punto già il Libro bianco sull'intelligenza artificiale del 19 febbraio 2020, cit., p. 23; nonché in dottrina, D. Amoroso, G. Tamburrini, *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?,* in *BioLaw Journal – Rivista di BioDiritto,* n. 1, 2019, p. 33; L. Parona, *Prospettive europee e internazionali di regolazione dell'Intelligenza artificiale tra principi etici, soft law e self regulation,* in *RRM*, n. 1, 2020, p. 70 ss.

dovrebbe tradursi, per il primo, nella possibilità di riesaminare le decisioni e i dati utilizzati per produrre un risultato, anche eventualmente superando la soluzione suggerita dal dispositivo di IA, alla luce delle caratteristiche del caso specifico; per il secondo, invece, nel diritto di essere informato delle diverse opzioni disponibili e nel diritto alla consulenza legale e all'accesso a un giudice.

6. *Riflessioni conclusive*

Gli sforzi compiuti dall'UE negli ultimi anni testimoniano la necessità di un cambiamento radicale per sfruttare appieno il potenziale degli strumenti digitali moderni, nel rispetto dei diritti fondamentali.

La crisi da COVID-19, come un'autentica cartina di tornasole, ha evidenziato sfide e rischi rispetto al funzionamento efficace dei sistemi giudiziari in circostanze eccezionali e ha sottolineato la necessità di rafforzare la resilienza dei sistemi giudiziari in tutta l'UE. Le Istituzioni UE hanno reagito, dando un nuovo impulso alla creazione di un approccio globale alla digitalizzazione della giustizia nell'UE, con lo scopo di cogliere tutte le opportunità possibili e assicurare al contempo garanzie adeguate.

È certamente troppo presto per provare a tracciare un bilancio sul se il recente intervento del legislatore UE potrà riuscire a rispondere in maniera efficace alle criticità che questa nuova tecnologia comporta quando viene impiegata nel settore della giustizia. Difatti, l'intera architettura regolatoria è attraversata da una profonda tensione tra due opposte esigenze e, cioè, da una parte, quella di cogliere le grandi opportunità che i sistemi di IA offrono e, dall'altra parte, quella di arginare i rischi che le tecnologie più avanzate comportano per i diritti e per le libertà fondamentali[70]. D'altronde, quando si parla di IA si fa riferimento ad una delle più promettenti tecnologie, rispetto alla quale è auspicabile la creazione di un mercato unico in cui si crei la più ampia facilitazione possibile alla produzione e alla ricerca, ma ci si rivolge altresì – e in questo sta l'ambivalenza – ad un complesso di strumenti a cui si accompagnano dei rischi di conseguenze negative, in particolare, per i diritti fondamentali[71].

[70] Per considerazioni diffuse sulla questione, si veda C. SCHEPISI, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale,* cit., pp. 53-75.

[71] Cfr. anche A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE*, 2023, p. 321 ss.

Invero, l'approccio orizzontale adottato dal legislatore lascia ancora margini di incertezza quando ci si interroghi sulle modalità applicative dei requisiti previsti allo specifico settore della giustizia.

Il carattere proporzionale dell'intervento umano che connota il nuovo regolamento, la cui variabilità in forma crescente discende dalle caratteristiche del contesto in cui è impiegata l'IA, nonché dall'entità delle conseguenze che l'impiego della stessa potrebbe provocare, denota certamente l'opzione per un'intelligenza artificiale complementare – piuttosto che sostitutiva – all'intelligenza umana, che permetta di garantire il rispetto dei valori fondamentali e dei principi su cui l'Unione si fonda. Ma, ad onta della previsione esplicita di obblighi gravanti su produttori e fornitori, non è dato sapere quali saranno in concreto il coinvolgimento, il ruolo e i doveri dei giudici e degli altri operatori del settore giudiziario nell'impiego di siffatta tecnologia.

In primo luogo, sembra sollevare qualche dubbio la stessa generica previsione delle applicazioni di IA individuate dal legislatore europeo, nel limite di quelle destinate «all'assistenza di un'autorità giudiziaria», senza ulteriormente chiarire cosa debba intendersi per «autorità giudiziaria».

Se si optasse per una interpretazione restrittiva si potrebbe circoscrivere la nozione all'«autorità in grado di fornire l'effettiva tutela giurisdizionale» garantita dall'art. 47 della Carta dei diritti fondamentali, ma tale lettura *stricto sensu* implicherebbe che, ad esempio, il lavoro di una Procura della Repubblica non rientri in questa specifica categoria ad alto rischio.

Un altro aspetto controverso, connesso alla previsione in esame, riguarda poi il fatto che lo stesso sistema di reperimento di informazioni legali o di ricerca della giurisprudenza, se utilizzato nella pratica privata (ad esempio, dagli avvocati), non sia considerato, almeno in teoria, ad alto rischio. In quest'ultimo caso, appare discutibile non solo che la diversa natura (privata) dell'utilizzatore, ma pur sempre operatore del settore, possa cambiare la categoria di rischio di tale sistema, ma anche che, se un sistema di IA, commercializzato esclusivamente per la pratica privata, seppure involontariamente utilizzato da un giudice, non soddisfi il requisito e quindi non sia considerato ad alto rischio.

Allo stesso modo, nonostante il regolamento prescriva, per l'addestramento delle macchine intelligenti, la necessità di utilizzare *set* di dati accessibili, sicuri, privi di errori e pregiudizi, permangono dubbi su quali azioni potranno essere realizzate in concreto per superare le criticità connesse al fenomeno delle *black box* e garantire che sia rispettato il dovere del giudice di motivare le sue decisioni, il principio di indipendenza e di imparzialità del giudice e il diritto ad una tutela giurisdizionale effettiva.

I problemi di scarsa trasparenza e oscurità del processo decisionale appaiono di fatto difficilmente compensabili dalle regole d'uso dei dati e/o dalle norme tecniche previste, soprattutto quando intervengano macchine come il *deep learning* basate su tecniche di autoapprendimento, il cui funzionamento non è intellegibile alla mente umana.

Per queste ragioni, sarà necessario individuare i possibili sviluppi del sistema giudiziario e identificare modelli compatibili con il rispetto dei diritti fondamentali.

Questa verifica si rivela particolarmente complessa in ragione del semplice fatto che gli strumenti algoritmici, sviluppati al di fuori del sistema giudiziario, creano una situazione inedita rispetto alla concezione classica del processo, in cui l'unico elemento esterno alle parti è il giudice. Nondimeno, i sistemi automatizzati sono tutt'altro che oggetti o attori neutrali, visto che la macchina che segue i passi di un algoritmo per raggiungere un risultato obbedisce a delle istruzioni esterne, rispetto alle quali non c'è alcuna garanzia che esse siano giuste o imparziali, e fare riferimento al concetto dell'*ethics by design* potrebbe non essere sufficiente.

In assenza di strumenti che consentano al giudice di comprendere il funzionamento del sistema utilizzato, allo stato, resta aperta la questione se questi sarebbe effettivamente in grado di discostarsi dalla decisione o dal suggerimento dell'IA qualora ce ne fosse bisogno, ancor più se si considera che il personale giudiziario, almeno allo stato, non dispone di un'adeguata formazione digitale che accresca la consapevolezza dell'impiego delle moderne tecnologie.

Al netto di tali dubbi, va osservato che il regolamento sull'IA, coerentemente con la sua vocazione, si limita a prevedere regole suscettibili di applicazione generale. Pertanto, le specifiche disposizioni, come quelle dell'amministrazione della giustizia, dovranno essere necessariamente accompagnate da altre regole puntuali e specificamente rivolte all'ambito in questione.

A tal fine, la strategia sull'IA della CGUE, che potrebbe essere in futuro inglobata in un atto vincolante, si presenta come un utile strumento di integrazione delle prescrizioni normative contenute nell'*AI Act* nello specifico settore della giustizia. Essa, infatti, più che un semplice insieme di linee guida, offre una visione lungimirante dell'integrazione delle moderne tecnologie nel settore in esame, imprimendo al percorso di rinnovamento dell'amministrazione della giustizia europea una precisa direzione.

In tal senso, il documento elaborato dalla Corte, da un lato, sottolinea la più ampia accettazione della tecnologia nell'amministrazione della giustizia,

dall'altro lato, individua in concreto le attività del settore che in funzione solo meramente tutoria potranno essere svolte con il supporto dell'IA. Essa, pertanto, rappresenta non solo un profondo cambiamento di prospettiva per una delle istituzioni tradizionalmente più conservatrici dell'UE, ma rappresenta anche un primo passo per promuovere l'uso responsabile dell'IA nei sistemi giudiziari degli Stati membri, in conformità con i valori dell'Unione europea.

Abstract (ita)

Il presente contributo si occupa della recente disciplina dell'Unione europea sull'Intelligenza artificiale, con specifico riferimento all'uso delle nuove tecnologie nel settore dell'amministrazione della giustizia. A tal fine, dopo una valutazione complessiva dei benefici e dei rischi dell'IA nel settore giudiziario, l'autore analizza le principali disposizioni dell'*AI Act* e offre una prima proiezione della loro applicazione al settore giudiziario alla luce dei principi di supervisione umana, trasparenza e non discriminazione.

Abstract (eng)

The paper deals with the recent EU framework on artificial intelligence, with specific reference to the use of new technologies in the field of administration of justice. To this end, after an overall assessment of the benefits and risks of AI in the judicial sector, the author analyses the main provisions of the AI Act and offers an initial screening of their application to the judicial sector in the light of the principles of human oversight, transparency and non-discrimination.

PRIME BREVI CONSIDERAZIONI SUL "DDL INTELLIGENZA ARTIFICIALE": INCOMPATIBILITÀ O INOPPORTUNITÀ?

Camilla Burelli[*]

SOMMARIO: 1. Premessa. – 2. L'AIA e la sua idoneità a regolare direttamente e immediatamente i rapporti giudici ad esso sottoposti. – 3. Il ddl recante disposizioni e delega al Governo in materia di intelligenza artificiale: una panoramica. – 4. I due (primi ed eventuali) profili di incompatibilità del ddl con il diritto dell'Unione europea. – 5. Qualche riflessione conclusiva sull'inopportunità (e l'intempestività) della misura nazionale.

1. *Premessa*

L'Unione europea, con l'adozione del regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act* – nel prosieguo "AIA"), approvato dal Parlamento europeo il 13 marzo 2024 e dal Consiglio il 21 maggio 2024[1], è uno dei primi ordinamenti giu-

[*] Ricercatrice (RTT) di Diritto dell'Unione europea presso l'Università degli Studi di Milano.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). V., tra i primi commenti, P. FRIEDL, G. G. GASIOLA, *Examining the EU's Artificial Intelligence Act*, in *verfassunblog.de*, 7 February 2024, che rilevano come «many of the decisions taken in the very final phase of the legislative process have rather weakened [the act] prospects»; T. MARKOFF, *The First of its Kind: the EU AI Act and What it Means for the Future of AI*, in *Fordham Journal of Corporate and Finantial Law – Blog*, 23 April 2024, che, al pari di P. Friedl e G. G. Gasiola, evidenzia come il successo del regolamento dipenderà in larga parte anche dall'efficacia delle sue (molte) misure di esecuzione. Illustra le principali tappe del percorso che ha portato all'adozione dell'AIA, N. T. NIKOLINAKOS, *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*, Berlin, 2023, spec. pp. 23-91 e p. 211 ss. In questo *fascicolo speciale* v. F. FERRI, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*; si occupa del ruolo degli *standard* armonizzati nell'attuazione dell'AIA, A. VOLPATO, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*; della tutela dei diritti fondamentali E. CIRONE, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*; delle c.d. *regulatory san-*

ridici a normare la materia *de qua*[2]. Peraltro, in data 23 aprile 2024, quindi a distanza di poco più di un mese dal "via libera" del Parlamento europeo, anche il Consiglio dei ministri italiano, su proposta della Presidente Giorgia Meloni e del Ministro della giustizia Carlo Nordio, ha approvato il disegno di legge (nel prosieguo "ddl") n. 1066AS per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale[3].

L'intelligenza artificiale e le sue implicazioni *lato sensu* giuridiche sono state oggetto, verosimilmente anche in ragione della loro estesa rilevanza mediatica, di una diffusa attenzione da parte della dottrina, sia italiana sia straniera[4]. Specialmente negli ultimi anni, infatti, se ne è vieppiù occupata la letteratura "comunitarista"[5]; ma anche internazionalista[6]; costituzionalista[7];

dboxes (e del rapporto tra l'AIA e il tema della co-regolazione) G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle regulatory sandboxes*.

[2] Lo evidenziano T. Markoff, *op. cit.*; A. Volpato, *op. cit.*, p. 2. M. Macchia, A. Mascolo, *Intelligenza artificiale e regolazione*, in A. Pajno, F. Donati, A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Bologna, 2022, p. 97 ss., spec. p. 98, giustamente scrivono: «[...] lo sviluppo di tali strumenti, tenuto conto delle implicazioni sociali, economiche e biologiche connesse all'utilizzo dell'intelligenza artificiale, non sembra poter essere affidato alle sole forze del mercato. Spetta al diritto il compito di regolare tale tecnologia, così da orientarne virtuosamente il funzionamento e declinarla al perseguimento delle finalità di interesse pubblico e sottese all'azione di legislatori e regolatori». Gli stessi Autori rilevano come l'attenzione dimostrata dall'Unione europea al tema dell'IA negli ultimi anni sia dovuta anche in risposta alla «corsa all'IA ingaggiata da USA e Cina», p. 104.

[3] Presentato in data 12 marzo 2024; annunciato nella seduta n. 168 del 13 marzo 2024, attualmente in corso di esame presso l'8^ Commissione permanente (Ambiente, transizione ecologica, energia, lavori pubblici, comunicazioni, innovazione tecnologica) del Senato.

[4] In dottrina è stato scritto che «[...] come sovente accade per gli argomenti che incrociano più discipline specialistiche e finiscono per essere di moda – la IA è, in un certo qual modo, vittima del proprio successo», v. S. Zorzetto, *La metafora della IA: una giungla lessicale e foresta simbolica*, in *POLITEIA*, 2023, p. 179 ss., spec. p. 180.

[5] V., ad esempio, M. C. Buiten, *Towards intelligent regulation of artificial intelligence*, in *European journal of risk regulation*, 2019, p. 41 ss.; C. Grieco, *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023; N. T. Nikolinakos, *op. cit.*; V. Salvatore (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, 2023.

[6] V., per tutti, B. Cappiello, *Ai-systems and non-contractual liability. A european private international law analysis*, Turin, 2022; J. Lee, *Artificial intelligence and international law*, Berlin, 2022, spec. pp. 139-218.

[7] V., *inter alia*, A. Simoncini, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 2019, p. 87 ss.; P. F. Bresciani, M. Palmirani, *Constitutional Opportunities and Risks of AI in the law-making process*, in

amministrativista[8]; penalista[9] e giuslavorista[10], solo per citare i principali settori dell'ordinamento giuridico in cui si è sviluppato e animato il dibattito attorno a questa giovane tematica (e senza naturalmente considerare i molti contributi di matrice filosofico-giuridica[11]).

In tale sede, lungi dal voler offrire un'approfondita analisi del contenuto e/o della portata del regolamento e del ddl, si intende piuttosto svolgere qualche riflessione sul rapporto che li lega. Si converrà, infatti, che la scelta del legislatore italiano di "anticipare" il legislatore "europeo" induce a interrogarsi, da un lato, sulla compatibilità della futura normativa nazionale con quella "comunitaria"[12] e, dall'altro lato, sulla sua opportunità "politi-

federalismi.it, 2024, p. 1 ss.

[8] V., *ex multis*, D.-U. Galetta, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in *federalismi.it*, 2023, p. 4 ss.

[9] V., tra i tanti, G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Diritto Penale Contemporaneo*, 2020, p. 75 ss.; G. Balbi, A. Esposito, S. Manacorda (a cura di), *Diritto penale e intelligenza artificiale. Nuovi scenari*, Torino, 2023.

[10] V., per tutti, C. Romeo, *L'era degli algoritmi e la sua incidenza nell'ambito della certezza del diritto: un connubio sospetto*, in *Il lavoro nella giurisprudenza*, 2024, p. 5 ss.

[11] V., ad esempio, P. Moro, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Rivista di diritto dei media*, 2019, p. 11 ss.; M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, in M. Ebers, S. Navas Navarro (eds.), *Algorithms and Law*, Cambridge, 2020, p. 37 ss.; S. Salardi, M. Saporiti (a cura di), *Le tecnologie 'morali' emergenti e le sfide etico-giuridiche delle nuove soggettività*, Torino, 2020; A. Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*, The Hague, 2022; G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022; S. Salardi, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, Torino, 2023.

[12] Sebbene l'aggettivo "comunitario" sia in parte desueto in parte financo scorretto, lo si usa per esigenze eufoniche. In argomento v. M. Condinanzi, *Da comunitario a unionale. La difficile ricerca di un aggettivo adatto*, in *EJ*, 10 aprile 2017. Recentemente, sollevano la medesima questione anche I. Anrò, J. Alberti, *Riflessioni sull'effetto diretto, sul primato e sulla disapplicazione del diritto nazionale*, in M. Graziadei, C. Iannone, B. Nascimbene, L. Salvato, E. Vincenti (coordinato da), *Il diritto europeo e il giudice nazionale*, Milano, 2023, p. 51 ss., spec. p. 52. M. Mastroianni, M. Condinanzi, *Giuseppe Tesauro – Advocate General at the ECJ (1988–1998): A Paladin of Effective Judicial Protection*, in D. Gallo, R. Mastroianni, F. G. Nicola, L. Cecchetti (eds.), *The Italian Influence on European Law. Judges and Advocates General (1952-2000)*, London, 2024, p. 153 ss., spec. p. 161, in corso di pubblicazione, ricostruiscono, invece, le ragioni dell'utilizzo di questo specifico aggettivo da parte del Prof. Giuseppe Tesauro anche dopo l'entrata in vigore del trattato di Lisbona: «Tesauro is the one who for many years rejected the use of the term 'union' and insisted on continuing to use the term 'community', in particular in the title of his already mentioned handbook ('Diritto comunitario'). He justified this choice in the light of the attention he wanted to reserve to the 'heart of the system', and the will to exclude what, for the citizen, belonged to the 'future or desirable', thereby showing a certain reluctance to purely formal matters».

co-legislativa".

Come noto, infatti, in ragione della natura dei regolamenti e della loro funzione nel sistema delle fonti, le disposizioni ivi contenute producono, in genere, effetti immediati negli ordinamenti giuridici degli Stati membri, senza che le autorità nazionali siano tenute ad adottare alcuna misura di attuazione[13]. È altrettanto noto, peraltro, che talune disposizioni possano richiedere, per la loro piena e corretta applicazione, l'adozione di misure di esecuzione da parte degli Stati membri[14] e, d'altro canto, è lo stesso art. 291, par. 1, TFUE a prevedere che «Gli Stati membri adott[i]no tutte le misure di diritto interno necessarie per l'attuazione degli atti giuridicamente vincolanti dell'Unione». Come autorevolmente scritto, «l'autosufficienza [del contenuto dispositivo dei regolamenti] è puramente eventuale, in vista della portata generale che è loro propria per definizione. È perciò esatto osservare che un regolamento può richiedere ulteriori apporti normativi – non essere quindi autosufficiente [...] – senza cessare per questo di essere direttamente applicabile»[15]. Gli Stati, quindi, possono adottare misure di attuazione di un regolamento se «non ostacolano la sua applicabilità diretta, se non dissimulano la sua natura di atto di diritto dell'Unione e se precisano l'esercizio del margine discrezionale ad essi conferito da[l] regolamento rimanendo nei limiti delle sue disposizioni»[16]. Il fatto che un regolamento affidi espressamente agli Stati membri la «cura di emanare le misure necessarie per la

[13] V., recentemente e per tutte, Corte giust. 21 marzo 2024, C-10/23, *Remia Com Impex*, punto 52. Naturalmente, tale caratteristica, *i.e.* l'effetto diretto, deriva dall'art. 288 TFUE, secondo cui il regolamento «è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri». In letteratura è stato scritto, con una certa forza evocativa, che «[...] la natura delle norme comunitarie autoapplicative rimaneva abbastanza misteriosa. La Corte aveva chiarito (richiamando alla nostra mente una famosa poesia di Eugenio Montale) che non si trattava né di diritto internazionale, né di diritto straniero, né di diritto interno. Anzi, a quest'ultimo proposito aveva vigorosamente chiarito come dovesse ritenersi illegittima qualunque pratica di nazionalizzazione delle norme in questione, soprattutto perché lesiva della competenza esclusiva della Corte di giustizia sancita dall'art. 177 del Trattato», v. G. Silvestri, *La diretta applicabilità delle norme comunitarie: implicazioni teoriche*, in AA. VV., *Annuario 1999: la costituzione europea. Atti del XIV Convegno annuale (Perugia, 7-8-9 ottobre 1999)*, Padova, 2000, p. 149 ss., spec. p. 155. Più in generale, in argomento, v. C. Amalfitano, M. Condinanzi, *Unione europea: fonti, adattamento e rapporti tra ordinamenti*, Torino, 2015, p. 52 ss.; I. Anrò, J. Alberti, *op. cit.*, pp. 59-60.

[14] V. sempre *Remia Com Impex*, sopra citata, punto 52.

[15] V. R. Luzzatto, *La diretta applicabilità nel diritto comunitario*, in R. Luzzatto, *Il diritto internazionale nella realtà dei fenomeni giuridici. Scritti scelti a cura degli allievi*, Torino, 2024, p. 1285 ss., spec. p. 1303.

[16] V. Corte giust. 12 aprile 2018, C-541/16, *Commissione/Danimarca*, punti 27 e 28.

sua attuazione» ha indotto a ritenere estensibile a questi la giurisprudenza dettata con riguardo alle direttive, in specie quella che impone che il giudice nazionale interpreti il proprio diritto nazionale quanto più possibile alla luce della lettera e dello scopo della direttiva per conseguire il risultato perseguito da questa[17].

Se, quindi, è pacifico che gli Stati membri sono abilitati a emanare, anche per i regolamenti, misure di esecuzione (e in effetti esse sono tendenzialmente contenute, con riguardo all'Italia, nella legge di delegazione europea[18]), è altrettanto vero che l'adozione di regole nazionali può, in potenza, determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori economico-giuridici, che, nel contesto che ci occupa, sono gli sviluppatori, gli importatori, i fornitori e gli utilizzatori di sistemi di IA. Ciò vale *a fortiori* se tale adozione dovesse avvenire "in via anticipata" rispetto all'intervento "comunitario". Infatti, sebbene il ddl debba essere (ancora) convertito in legge, come meglio si vedrà *infra*, § 5, è verosimile che ciò avvenga *prima* dell'effettiva applicazione del regolamento, che, ai sensi dell'art. 113 AIA, inizierà a decorrere dal 2 agosto 2026[19].

[17] V. conclusioni dell'Avv. gen. Mischo, del 30 marzo 2000, C-403/98, *Monte Arcosu*, parr. 70 e 71, che citava espressamente giurisprudenza relativa a direttive (su tutte Corte giust. 13 novembre 1990, C-106/89, *Marleasing*, punto 8), affermando peraltro che, sebbene si trattasse di direttive piuttosto che di un regolamento, com'era nel caso di specie, ciò non rilevava. Dato che il regolamento affidava espressamente agli Stati membri il compito di adottare misure per la sua applicazione, infatti, non occorreva distinguerlo da una direttiva ai fini dell'applicazione di tale giurisprudenza.

[18] Sebbene non sia questa la sede per approfondimenti, la legge di delegazione europea è, insieme alla legge europea, uno dei due strumenti di adeguamento all'ordinamento dell'Unione introdotti dalla già legge 24 dicembre 2012, n. 234, che ha attuato una riforma organica delle norme che regolano la partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione. L'art. 30, comma 2, lett. e), della legge prevede che la legge di delegazione europea reca, *inter alia*, la «delega legislativa al Governo limitata a quanto necessario per dare attuazione a eventuali disposizioni non direttamente applicabili contenute in regolamenti europei». Si noti che l'art. 37 della medesima legge dispone che possano essere adottati provvedimenti, anche urgenti, diversi dalla legge di delegazione europea e dalla legge europea, necessari a fronte di atti normativi UE o di sentenze della Corte ovvero dell'avvio di procedure di infrazione che comportano obblighi statali di adeguamento, qualora il termine per provvedervi risulti anteriore alla data di presunta entrata in vigore della legge di delegazione europea o della legge europea relativa all'anno di riferimento. In dottrina, *ex plurimis*, v. M. ROSINI, *Legge di delegazione europea e legge europea. Contributo allo studio dell'attuazione del diritto dell'Unione europea nel più recente periodo*, Napoli, 2017.

[19] Salvo i capi I e II che si applicheranno a partire dal 2 febbraio 2025; il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'art. 78, invece, si applicano a decorrere dal 2

In ogni caso, a prescindere da tale *dies a quo* e dall'eventuale necessità di misure di applicazione, il regolamento produce *comunque* effetti immediati all'interno degli Stati membri[20].

Tali considerazioni impongono, dunque, di esaminare la legittimità delle disposizioni del ddl italiano, che, per un verso, potrebbero ostacolare l'efficacia diretta del regolamento UE, compromettendone la (futura) simultanea e uniforme applicazione[21] e, per altro verso, potrebbero presentare eventuali profili di incompatibilità, meno "di sistema" e più strettamente "tecnici". Infatti, sebbene sia probabile che il testo della misura nazionale muti per tenere conto del regolamento *medio tempore* entrato in vigore, ciò non toglie che la manovra resta, sul piano politico, poco comprensibile. Allo scopo, quindi, è necessario dare brevemente conto dei caratteri fondamentali dei provvedimenti *de quibus*, avendo cura di evidenziare, in particolare, le disposizioni relative all'applicazione e, dunque, all'esecuzione del regolamento (§§ 2 e 3). Dopodiché, si enucleeranno i primi ed eventuali profili di incompatibilità del ddl con il diritto dell'Unione europea (§ 4). Per concludere, infine, si svolgeranno brevi riflessioni sull'inopportunità (e l'intempestività) della misura nazionale (§ 5).

2. *L'AIA e la sua idoneità a regolare direttamente e immediatamente i rapporti giudici ad esso sottoposti*

Dedicare all'intero AIA qualche parola riassuntiva sarebbe, in questa sede, assai difficile e non renderebbe giustizia alla ricchezza e alla complessità (anche di formulazione) delle disposizioni ivi contenute[22]. Di seguito, quindi, dopo

agosto 2025, ad eccezione dell'art. 101. L'art. 6, par. 1, e i corrispondenti obblighi di cui al regolamento, infine, si applicheranno addirittura a decorrere dal 2 agosto 2027.

[20] V., oltre alla giurisprudenza citata *supra*, nota 13, Corte giust. 14 aprile 2011, C-42/10, C-45/10 e C-57/10, *Vlaamse Dierenartsenvereniging e Janssens*, punto 48; più di recente, v. anche le conclusioni dell'Avv. gen. Szpunar, dell'11 maggio 2023, C-33/22, *Österreichische Datenschutzbehörde*. Si noti, peraltro, che, come noto, se il regolamento prevede l'adozione di misure di applicazione da parte degli Stati membri, a cui è riconosciuto un certo margine di discrezionalità, e le sue disposizioni non risultino sufficientemente precise, i singoli non possono azionare diritti sulla base del solo regolamento. V., in proposito, Corte giust. 11 gennaio 2001, C-403/98, *Monte Arcosu*, punto 28. V. anche le conclusioni dell'Avv. gen. Wahl, del 4 maggio 2017, C-183/16 P, *Tilly-Sabco/Commissione*, par. 58.

[21] V., in questi termini, per tutte, Corte giust. 7 febbraio 1973, 39/72, *Commissione/Italia*, punto 17.

[22] Il regolamento consta di centoottanta considerando, centrotredici articoli suddivisi in

aver brevemente ricordato qual è la nozione di intelligenza artificiale che il regolamento abbraccia e dopo averne tratteggiato le principali linee direttrici, si concentrerà l'attenzione sugli articoli relativi alla sua applicazione, valutandone l'idoneità a regolare direttamente e immediatamente i rapporti giudici e ponendoli, quindi, in relazione alle disposizioni contenute nel ddl italiano.

Secondo l'AIA – che, come efficacemente scritto, «è figlio del pensiero illuminista che ripone incondizionata fiducia nella capacità predittiva della macchina e nelle virtù previsionali dell'uomo, che saprà disegnare regole anticipatorie, well tailored sul rischio, e idonee a impedirne l'avveramento»[23] – l'intelligenza artificiale «consiste in una famiglia di tecnologie in rapida evoluzione che può contribuire al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali»[24]. Un "sistema di IA", invece, è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[25]. Con riguardo, ancora, all'obiettivo del regolamento – che, come risulta dal considerando n. 1, è invero piuttosto articolato e complesso e suggerisce l'ampio ventaglio di situazioni giuridiche a cui si applica l'AIA e, quindi, l'estensione del suo ambito oggettivo – esso mira a istituire un quadro giuridico uniforme in materia di IA per regolare lo sviluppo, l'immissione sul mercato, la messa in servizio, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza, la protezione dei valori dell'Unione europea e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'UE ("Carta"). Sempre su un piano generale, il regolamento contribuisce, poi, all'obiettivo di promuovere l'approccio «antropocentrico europeo» all'IA e a rendere l'Unione «un *leader* mondiale nello sviluppo

tredici capi (nell'ordine: disposizioni generali; pratiche di intelligenza artificiale vietate; sistemi di IA ad alto rischio; obblighi di trasparenza per i fornitori e i *deployer* di determinati sistemi di IA; modelli di IA per finalità generali; misure a sostegno dell'innovazione; *governance*; banca dati dell'UE per i sistemi di IA ad alto rischio; monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni, vigilanza del mercato; codici di condotta e orientamenti; delega di potere e procedura di comitato; sanzioni; disposizioni finali) e tredici allegati.

[23] Così G. De Minico, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, 29 aprile 2024, p. 1 ss., spec. p. 3.

[24] Cfr. il considerando n. 4 dell'AIA.

[25] *Ibidem*, art. 3, par. 1, n. 1.

di un'IA sicura, affidabile ed etica»[26].

Con riguardo alla classificazione dei sistemi di IA[27] e alle pratiche di IA vietate, seguendo un approccio basato sul rischio – il medesimo abbracciato dal regolamento sulla protezione dei dati personali[28] – in virtù del quale al crescere del rischio cresce il rigore delle regole[29], l'AIA stabilisce obblighi per fornitori e operatori dei sistemi di IA a seconda, appunto, del livello di rischio che l'IA può comportare: a) un rischio inaccettabile; b) un rischio alto; c) un rischio limitato, minimo o nullo. Nel primo caso le pratiche di IA collegate sono assolutamente vietate (l'art. 5, par. 1, lett. f), "bandisce", ad esempio, i sistemi di riconoscimento delle emozioni utilizzati sul luogo di lavoro e negli istituti scolastici); nel secondo caso sono ammesse nei limiti in cui il bilanciamento tra innovazione e tutela delle libertà fondamentali sia in grado di minimizzare il rischio (ad esempio, l'allegato III, che precisa i sistemi di IA ad alto rischio *ex* art. 6, par. 2, menziona quelli finalizzati all'individuazione, al riconoscimento o all'identificazione delle persone nel contesto della migrazione, dell'asilo o della gestione delle frontiere); nel terzo caso, le attività presentano un rischio così lieve da essere esentate dall'osservanza delle regole più gravose (si pensi, con riguardo ai sistemi di IA dal rischio limitato, ai c.d. "*deep fake*"[30]; mentre, con riguardo ai sistemi dal rischio nullo,

[26] *Ibidem*, considerando n. 8.

[27] Nell'originaria proposta della Commissione, i sistemi di IA erano definiti, all'art. 3, par. 1, n. 1, come «*software* sviluppati con una o più delle tecniche e degli approcci elencati nell'allegato I, che [possono], per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

[28] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). In argomento v., per tutti, R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020; M. Krzysztofek, *GDPR: Personal Data Protection in the European Union*, Alphen aan den Rijn, 2021, in particolare il capitolo 12.

[29] V., a tal proposito, quanto sinteticamente affermato al considerando n. 26, che recita: «Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA».

[30] L'art. 50 del regolamento pone alcuni obblighi di trasparenza ai fornitori dei sistemi di IA destinati a interagire direttamente con le persone, stabilendo che siano «progettati e

ai filtri *spam*). Il rischio dell'IA pare essere, quindi, un «attributo fisiologico della fattispecie»[31], tenuto in considerazione dal legislatore UE che, in effetti, ha evidentemente scelto un modello regolatorio di tipo «precauzionale»[32].

Tanto premesso, il regolamento, che disciplina l'IA dalla sua creazione sino alla sua eventuale rimozione dal mercato[33], si affida ampiamente alle future misure di attuazione della Commissione europea, che è incaricata, da un lato, di dettagliare e specificare alcuni aspetti della disciplina e, dall'altro lato e soprattutto, di aggiornarla e rinnovarla sulla base della fisiologica evoluzione tecnologica. È pertanto prevista l'adozione di atti delegati (ad esempio, per aggiungere criteri di classificazione dei modelli di IA per finalità generali come modelli che presentano rischi sistemici, come disposto dall'art. 51) e di atti esecutivi (ad esempio, secondo l'art. 50, per approvare o specificare eventuali codici di buone pratiche a livello UE per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei

sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo».

[31] Così sempre G. De Minico, *op. cit.*, p. 2.

[32] *Ibidem*, p. 2. F. Ferri, *op. cit.*, p. 18, riprendendo G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, 2022, p. 473 ss., scrive che il regolamento «[...] si fonda su un "*top-down risk approach*", evincibile già nella fase di valutazione».

[33] Le disposizioni ivi contenute, infatti, siano esse formulate in modo *soft* o *hard*, normano la scelta degli elementi che compongono uno specifico sistema di IA, l'addestramento dei dati e la loro conservazione, la valutazione e la verifica degli *input* e degli *output*, l'eventuale intervento umano, l'immissione del sistema nel mercato e la sua "manutenzione" (*i.e.*, l'aggiornamento e il monitoraggio), così come il suo ritiro dal mercato qualora esso comporti dei danni irreversibili. La nuova disciplina, che prevede alcune eccezioni alla sua applicazione per le forze dell'ordine in circostanze chiaramente identificate, contiene anche alcune misure a sostegno dell'innovazione. In particolare, consente la creazione di spazi di sperimentazione normativa per l'IA (c.d. *sandbox* normativi) e di prova in condizioni reali, che forniscono un ambiente controllato per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle *start-up*. Con riguardo alle IA già immesse sul mercato, il regolamento concede un periodo di quattro anni alle autorità pubbliche fornitrici o utilizzatrici di sistemi di IA ad alto rischio per rendere conformi i propri sistemi; il periodo si riduce a tre anni per i modelli GPAI immessi sul mercato prima della data di applicazione delle disposizioni a loro relative (ossia due anni a partire da dodici mesi dopo l'entrata in vigore del regolamento). Infine, le sanzioni per le violazioni della nuova disciplina sono state calcolate in una percentuale del fatturato annuo globale nell'anno finanziario precedente della società autrice della violazione o in un importo predeterminato, a seconda di quale sia il più elevato.

contenuti generati o manipolati artificialmente) da adottarsi *ex* artt. 290 e 291 TFUE. Sul punto è stato efficacemente scritto che «[s]i tratta di attribuzioni certamente rilevanti e che vanno ben oltre la capillarità degli orientamenti attuativi che la Commissione può produrre [in forza dell'art. 96 AIA]. Effettivamente, la Commissione è nelle condizioni di incidere profondamente sull'operatività dell'AIA, che in assenza di queste misure rischierebbe di risultare inefficace»[34].

Ampio spazio di manovra, peraltro, è lasciato anche agli Stati membri. D'altro canto, sebbene in questo contesto la diretta applicabilità abbia «il compito di far progredire [...] l'integrazione, di fronte agli ostacoli di natura politica»[35], ma anche e soprattutto di natura tecnologica, è lo stesso regolamento, al considerando n. 153, a dichiarare che «[g]li Stati membri svolgono un ruolo chiave nell'applicare ed eseguire il presente regolamento»[36]. Anche nella relazione di accompagnamento della proposta di regolamento presentata dalla Commissione, era scritto che «le disposizioni del regolamento *non sono eccessivamente prescrittive* e *lasciano spazio a diversi livelli di azione da parte degli Stati membri* in relazione ad aspetti che non pregiudicano il conseguimento degli obiettivi dell'iniziativa»[37].

A tal proposito, si pensi, a mero titolo esemplificativo, all'art. 5, che disciplina le pratiche di IA vietate: al paragrafo 3, la norma dispone che l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto «è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e *in conformità delle regole det-*

[34] V. F. Ferri, *op. cit.*, p. 4.

[35] Usa queste parole R. Luzzatto, *op. cit.*, p. 1286.

[36] Anche M. Macchia, A. Mascolo, *op. cit.*, p. 117, certo con riferimento alla proposta di regolamento presentata dalla Commissione, rilevano che «[...] ampio spazio di azione [è lasciato agli] Stati membri». M. Inglese, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in questo *fascicolo speciale*, spec. p. 16, invece, osserva che la scelta di usare il regolamento è chiaramente intesa a evitare che gli Stati membri compromettano, con eventuali spazi di manovra a loro così negati, l'approccio unitario ai profili delle nuove tecnologie. In verità, sebbene evidentemente sempre di un regolamento si tratta, si ritiene che gli spazi di manovra lasciati agli Stati membri non siano così trascurabili.

[37] V. relazione di accompagnamento alla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, Bruxelles, 21 aprile 2021, COM (2021) 206final, spec. punto 2.4 (corsivo aggiunto).

tagliate del diritto nazionale»[38]. Il paragrafo 5 della medesima norma prevede, poi, che uno Stato membro «[possa] 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» e, a tal fine, deve «stabili[re] nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative». Ancora, l'art. 28, che impone che ciascuno Stato membro designi o istituisca almeno un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e del monitoraggio dei sistemi di IA ad alto rischio, prevede altresì che gli Stati membri siano liberi di decidere se tali attività debbano essere eseguite da un organismo nazionale di accreditamento ai sensi del regolamento (CE) n. 765/2008, cioè il regolamento che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti[39].

Sempre a titolo esemplificativo, si pensi ancora all'art. 57, che dispone che siano gli Stati membri a provvedere affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale. L'art. 62, rubricato «*Misure per i fornitori e i* deployer*, in particolare le PMI, comprese le start-up*» enuclea tutta una serie di azioni che gli Stati membri devono intraprendere a favore di questi soggetti, come, ad esempio, organizzare specifiche attività di sensibilizzazione e formazione sull'applicazione del regolamento adattate alle esigenze delle PMI, comprese le *start-up*, degli utenti e, se del caso, delle autorità pubbliche locali o, ancora, istituire canali per la comunicazione con i predetti soggetti al fine di fornire consulenza e rispondere alle domande sull'attuazione del regolamento. Gli Stati membri, poi, ai sensi dell'art. 70, par. 2, devono designare un'autorità di vigilanza del mercato che funga da punto di contatto unico per il regolamento e devono garantire che le loro autorità nazionali competenti, che devono dotarsi di un adeguato livello di misure di cibersicurezza, dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti a norma del regolamento (è il considerando n. 153 a stabilire che è opportuno che ciascuno Stato designi almeno una autorità di notifica e almeno una autorità

[38] Corsivo aggiunto.

[39] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93.

di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del regolamento).

Anche la disciplina dei codici di condotta, in specie l'art. 95, parr. 1 e 2, lascia ampi spazi di azione agli Stati membri. Il primo paragrafo dispone che «gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta [...]»; il secondo che «gli Stati membri agevolano l'elaborazione di codici di condotta relativi all'applicazione volontaria, anche da parte dei *deployer*, di requisiti specifici a tutti i sistemi di IA, sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi [...]».

Nei considerando del regolamento si legge, invece, che al fine di assicurare un quadro giuridico che promuova l'innovazione, gli Stati membri «dovrebbero garantire che le rispettive autorità nazionali competenti istituiscano almeno uno spazio di sperimentazione normativa in materia di IA a livello nazionale per agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio» (considerando n. 138); o, ancora, che gli Stati membri sono «incoraggiati» a sostenere e promuovere la ricerca e lo sviluppo di soluzioni di IA a sostegno di risultati vantaggiosi dal punto di vista sociale e ambientale, come le soluzioni basate sull'IA per aumentare l'accessibilità per le persone con disabilità (considerando n. 142). Ogni Stato membro, poi, dovrebbero «stabilire» la normativa relativa alle sanzioni, comprese le sanzioni amministrative pecuniarie (considerando n. 179).

Il regolamento fa financo salve due ipotesi di *gold-plating* "autorizzato" (autorizza espressamente, cioè, l'adottabilità di misure più stringenti rispetto a quelle di derivazione "comunitaria" e, quindi, per tale ragione, non è *gold-plating* in senso stretto[40]): l'art. 5, par. 5, infatti, prevede che gli Stati membri possano introdurre, in conformità con il diritto UE, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota *a posteriori*; e anche l'art. 2, par. 11, non osta «a che gli Stati mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi

[40] Se si assume che il *gold-plating* sia, in sintesi, un eccesso di regolamentazione da parte del legislatore nazionale rispetto a quanto richiesto e imposto dal diritto UE, va da sé che, se l'eccesso di regolamentazione è, per l'appunto, ammesso dallo stesso diritto UE, non si è in presenza di *gold-plating* in senso stretto. In argomento, sia concesso rinviare a C. Burelli, *Il gold plating e l'armonizzazione "spontanea", due tecniche legislative a confronto*, in *RIDPC*, 2022, p. 617 ss., spec. p. 637.

di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contratti collettivi più favorevoli ai lavoratori».

Infine, pare opportuno ricordare che, in virtù dell'art. 4, par. 2, TUE e delle specificità della politica di difesa comune degli Stati membri e dell'Unione, il regolamento stabilisce che, nella misura in cui i sistemi di IA siano immessi sul mercato, messi in servizio o utilizzati per scopi militari, di difesa o di sicurezza nazionale, essi restano (evidentemente) esclusi dall'ambito di applicazione del regolamento, indipendentemente dal tipo di entità che svolge tali attività, ad esempio se si tratta di un'entità pubblica o privata.

Più in generale, comunque, e a prescindere dalle disposizioni che attribuiscono espressamente poteri più o meno discrezionali agli Stati membri, il regolamento sembra fare uso, talvolta, di concetti a tratti indeterminati, a tratti suscettibili di interpretazione, con il rischio di applicazioni difformi all'interno del territorio dell'Unione[41]. Si pensi, ad esempio, alla disciplina in materia di pratiche di IA vietate: l'art. 5, par. 2, stabilisce che «[l]'uso di sistemi di identificazione biometrica remota "in tempo reale"[42] in spazi ac-

[41] In questo senso, certo con riferimento alla proposta della Commissione, che comunque non è mutata su tale specifico punto, v. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2022, p. 415 ss., spec. pp. 422-423, che scrivono: «La presenza di concetti indeterminati ed interpretabili implica flessibilità applicativa e, di conseguenza margini di manovra a favore degli Stati membri. D'altro canto, in mancanza di pratiche applicative comuni, il rischio è che tale indeterminatezza generi anche incertezza, aprendo la possibilità di applicazioni difformi della disciplina all'interno del territorio dell'Unione e un conseguente aumento del contenzioso giudiziario». Evidenzia il medesimo problema legato all'uso di definizioni poco chiare e di un approccio eccessivamente "sfumato" («*nuanced*») anche J. LEVANO, *Predictive Policing in the AI Act: meaningful ban or paper tiger?*, in *European Law Blog*, 5 July 2024, che tratta la questione con riferimento alle disposizioni in materia di c.d. "*predictive policing*" (*ie*, polizia predittiva) e di identificazione dei potenziali criminali. Per una ricostruzione delle varie definizioni del concetto di "*predictive policing*", v. I. MUGARI, E. OBIOHA, *Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing*, in *Social Sciences*, 2021, p. 3 ss.

[42] Ai sensi dell'art. 3, par. 1, n. 42, per sistema di identificazione biometrica remota "in tempo reale" si intende «un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi e in cui sono incluse non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione della normativa»; a sua volta, ai sensi del medesimo articolo, par. 1, n. 41, un sistema di identificazione biometrica remota è «un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento».

cessibili al pubblico [...], è applicato solo [...] per confermare l'identità della persona specificamente interessata e tiene conto dei seguenti elementi: a) la natura della situazione che dà luogo al possibile uso, in particolare *la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema*»[43]. È chiaro che l'impiego di termini generici e indeterminati come «gravità», «probabilità», «entità» del danno, così come di locuzioni indefinite come «che sarebbe causato in caso di mancato uso del sistema», la cui valutazione spetterebbe evidentemente all'autorità giudiziaria o all'autorità amministrativa, può generare incertezza giuridica sulla corretta interpretazione e applicazione della disposizione[44].

Queste norme – menzionate, lo si ripete, a mero titolo esemplificativo – mostrano chiaramente come il regolamento (a prescindere dalla politica di difesa comune) lasci, su più di un fronte, un indiscusso potere discrezionale a favore degli Stati membri, che, da questo punto di vista, hanno dinnanzi a sé un atto che, per certi versi, somiglia più a una direttiva che non a un regolamento in senso stesso, per sua natura idoneo a regolare direttamente e immediatamente (tutti) i rapporti giudici ad esso sottoposti. Ci si può quindi legittimamente chiedere se queste disposizioni, pur imponendo agli Stati membri determinati obblighi, risultino effettivamente idonee a essere concretamente applicate dal giudice interno[45] o dalle pubbliche amministrazioni. La sensazione è che, lungi dall'essere autosufficienti, alcune di queste norme si avvicinino, talvolta, più che altro a dei «programmi di legislazione»[46] e, in fondo, il largo affidamento agli atti delegati e di esecuzione della Commissione, così come all'ulteriore intervento legislativo o amministrativo da parte degli Stati membri, sembra dimostrarlo.

Prima di procedere, peraltro, all'analisi delle conseguenze di tale scelta legislativa, in specie le sue implicazioni sul rapporto con il recente ddl in materia di intelligenza artificiale, pare opportuno enucleare brevemente quali sono le principali disposizioni contenute in quest'ultimo atto nazionale.

[43] Corsivo aggiunto.

[44] Svolgono simili considerazioni sempre C. CASONATO, B. MARCHETTI, *op. cit.*, p. 422.

[45] In argomento v., *amplius*, P. MENGOZZI, *Diretta applicabilità del diritto comunitario, poteri del giudice ordinario e decisioni della commissione CEE*, in *Contratto e impresa*, 1990, p. 56 ss.

[46] Usa questa espressione R. LUZZATTO, *op. cit.*, p. 1286.

3. *Il ddl recante disposizioni e delega al Governo in materia di intelligenza artificiale: una panoramica*

Il ddl recante disposizioni e delega al Governo in materia di intelligenza artificiale, che si articola in quattro capi per un totale di ventisei articoli, si pone anzitutto il problema di precisare il suo campo di applicazione. L'art. 1, rubricato "*Finalità e ambito di applicazione*", stabilisce che la legge «[r]eca principi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e modelli di intelligenza artificiale», promuovendo un utilizzo corretto, trasparente e responsabile, «in una dimensione antropocentrica» dell'intelligenza artificiale (al pari del regolamento, che, ugualmente, intende promuovere la diffusione di un'IA antropocentrica e affidabile, come dichiarato al considerando n. 1), volto a coglierne le opportunità. Garantisce, poi, la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'intelligenza artificiale. Il tutto dovendosi interpretare e applicare «conformemente al diritto dell'Unione europea».

Opera, poi, uno sforzo definitorio di nozioni invero già introdotte con il regolamento "comunitario". Un sistema di intelligenza artificiale sarebbe infatti, esattamente come previsto dall'AIA, «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali». Parzialmente diversa, invece, è la nozione di "modello di IA". Se nel ddl questo è definito come un «modell[o] che identific[a] strutture ricorrenti attraverso l'uso di collezioni di dati, che *hanno la capacità di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni*»[47], nel regolamento esso è descritto, all'art. art. 3, par. 1, n. 63, come «un modello di IA [...] addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia *in grado di svolgere con competenza un'ampia gamma di compiti distinti*, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e *che può essere integrato in una varietà di sistemi o applicazioni a valle*, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione

[47] Corsivo aggiunto.

prima di essere immessi sul mercato»[48]. La norma "comunitaria", poi, parla di modello di IA «per finalità generali» e non solo di «modello di IA», come accade a livello nazionale.

Il principio – l'«approccio», per dirla con l'art. 3 del ddl – a cui si ispira l'intera misura è, comunque, quello «proporzionale e basato sul rischio» gemello dell'AIA.

Il ddl, dopo aver enunciato i principi che ispirano la materia dell'informazione della riservatezza dei dati personali e dello sviluppo economico (rispettivamente, artt. 4 e 5), si occupa di dettare disposizioni di dettaglio nei settori (*i*) della sicurezza e della difesa nazionale (art. 6); (*ii*) della sanità (artt. 7-9); (*iii*) del lavoro (artt. 10-12); (*iv*) della pubblica amministrazione; (*v*) dell'attività giudiziaria (art. 14); (*vi*) della cybesicurezza (art. 16). Predispone, poi, la strategia nazionale per l'intelligenza artificiale (art. 17); designa le autorità nazionali per l'intelligenza artificiale (art. 18); autorizza alcune spese finalizzate alla realizzazione di progetti sperimentali volti all'applicazione dell'intelligenza artificiale ai servizi forniti dal Ministero degli affari esteri e della cooperazione internazionale a cittadini e a imprese (art. 19); pone alcune misure di sostegno a favore dei giovani e dello sport (art. 20); autorizza una serie di investimenti nei settori dell'IA, della cybersicurezza e del calcolo quantistico (art. 21); delega il Governo all'adozione di uno o più decreti legislativi per l'adeguamento della normativa nazionale all'AIA (art. 22); pone alcune disposizioni a tutela degli utenti e in materia di diritto d'autore (artt. 23-24); introduce talune modifiche al codice penale (art. 25) e al codice civile (art. 15) e, infine, impone che dall'attuazione della legge non derivino nuovi o maggiori oneri a carico della finanza pubblica (art. 26).

In questa sede, lungi dal voler illustrare ciascuna delle disposizioni testé menzionate, operazione che uscirebbe dall'oggetto del presente lavoro, ci si limiterà a mettere in evidenza quelle che presentano un rapporto più stretto con quanto disciplinato (o non disciplinato) dall'AIA, rinviando al testo del disegno di legge per quanto non espressamente menzionato nel prosieguo.

Come anticipato, il ddl si occupa (legittimamente) di dettare disposizioni nel settore della sicurezza e difesa nazionale. Tuttavia, le attività di cui all'art. 3, comma 1 (*ie* la ricerca, la sperimentazione, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di IA) svolte per scopi di sicurezza nazionale, di cybersicurezza nonché quelle svolte per scopi di difesa nazionale dalle forze armate, sono escluse dall'ambito applicativo della emananda legge. Le medesime attività sono comunque effettuate, dispone il ddl, «nel

[48] Corsivi aggiunti.

rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione e di quanto disposto dall'art. 3, comma 4», cioè senza pregiudicare lo svolgimento con metodo democratico della vita istituzionale e politica.

L'art. 7 del ddl disciplina l'uso dell'intelligenza artificiale in ambito sanitario e di disabilità[49], mentre gli artt. 8 e 9 regolano, rispettivamente, la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario e la formazione del fascicolo sanitario elettronico, i sistemi di sorveglianza e il governo della sanità digitale. L'art. 7 – qui l'unico che verrà illustrato per la sua portata più ampia – prevede, al secondo comma, che l'introduzione di sistemi di intelligenza artificiale nel sistema sanitario non può «selezionare e condizionare l'accesso alle prestazioni sanitarie con criteri discriminatori», mentre, al terzo comma, che l'interessato ha diritto di essere informato «circa l'utilizzo di tecnologie di IA e sui vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie, nonché di ricevere informazioni sulla logica decisionale utilizzata». La disposizione, poi, pur riconoscendo che i sistemi di IA in ambito sanitario costituiscono un supporto alla prevenzione, alla diagnosi, alla cura e alla scelta terapeutica, prescrive che la decisione finale è sempre rimessa alla professione medica e, per tale ragione, deve restare impregiudicata. L'art. 7, comma 6, impone, infine, che i dati impiegati in ambito sanitario «devono essere affidabili e periodicamente verificati e aggiornati al fine di minimizzare il rischio di errori».

Il regolamento, dal canto suo, con riguardo al settore sanitario, oltre a qualche dichiarazione di principio contenuta nei considerando nn. 47[50],

[49] In materia di IA e tutela salute, è stato scritto che «[s]iamo di fronte a una vera e propria rivoluzione, che presenta peraltro non pochi rischi, in considerazione della rilevanza e della sensibilità dei dati relativi alla salute degli individui, delle esigenze di tutela della riservatezza, dei profili di responsabilità medica e delle possibili distorsioni cognitive dovute ad assunzioni errate nel processo di apprendimento automatico», v. V. SALVATORE, *L'Unione europea disciplina l'impiego dell'intelligenza artificiale e dei processi di digitalizzazione anche al fine di promuovere la tutela della salute*, in V. SALVATORE (a cura di), *op. cit*., p. 3 ss., spec. p. 4.

[50] Il considerando n. 47 recita: «Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati».

58[51] e 68[52], si limita a stabilire, all'art. 59, rubricato «*Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico*» e caratterizzato da una formulazione invero "infelice", che i dati personali legalmente raccolti possono essere trattati nello spazio di sperimentazione normativa per l'IA unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando sono soddisfatte, *inter alia*, tali condizioni: «la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari [...]». L'allegato III, poi, inserisce tra i sistemi di IA ad alto rischio di cui all'art. 6, par. 2, quelli destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità, la concessione, la riduzione, la revoca o il recupero, per le persone fisiche, delle prestazioni e dei servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria.

Come anticipato, gli artt. da 10 a 12 disciplinano, con un approccio di natura sempre antropocentrica, l'utilizzo dell'IA in materia di lavoro. L'art. 10 stabilisce che l'intelligenza artificiale deve essere impiegata per migliorare le condizioni di lavoro, tutelare l'integrità psico-fisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone «in conformità al diritto dell'Unione europea» (art. 10). Per quanto qui rileva, il legislatore italiano ha altresì sancito un obbligo di informativa a carico del datore di lavoro o committente che utilizzi sistemi di IA, in tal modo

[51] Il considerando n. 58 recita: «Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni servizi e prestazioni essenziali, pubblici e privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. In particolare, le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, vale a dire servizi sanitari, sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità competenti. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere concessi, negati, ridotti, revocati o recuperati dalle autorità, compreso se i beneficiari hanno legittimamente diritto a tali prestazioni o servizi, possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana o a un ricorso effettivo e dovrebbero pertanto essere classificati come sistemi ad alto rischio».

[52] Il considerando n. 68 recita: «Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di IA a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata *governance* istituzionale».

estendendo la casistica di cui all'art. 1-*bis* del d.lgs. n. 152/1997[53]. L'art. 11 impone che l'utilizzo dell'IA avvenga nel rispetto dei diritti fondamentali dei lavoratori, evitando discriminazioni basate sul sesso, l'età, l'origine etnica, il credo religioso, le opinioni politiche e le condizioni personali, sociali ed economiche, con ciò mirando a contrastare la c.d. "discriminazione algoritmica", ovvero la produzione di errori nei sistemi di IA che falsino l'elaborazione degli *input* e generino *output* discriminatori, appunto, per i lavoratori[54].

L'AIA, che lascia impregiudicate le normative nazionali in materia di lavoro[55], al già menzionato allegato III inserisce, tra i sistemi di IA ad alto rischio di cui all'art. 6, par. 2, anche quelli destinati a essere utilizzati, da un lato, per l'assunzione o la selezione di persone fisiche e, dall'altro lato, per adottare decisioni riguardanti «le condizioni dei rapporti di lavoro, la promozione o la cessazione di questi, e per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali dei lavoratori».

Con un approccio chiaramente antropocentrico e precauzionale, l'art. 14 del ddl disciplina l'impiego dell'IA nell'attività giudiziaria. Esso stabilisce che i sistemi di IA sono utilizzati «*esclusivamente*»[56] per l'organizzazione e la semplificazione del lavoro giudiziario nonché per la ricerca giurisprudenziale e dottrinale e, al pari dell'ambito sanitario, anche in tale contesto «[è] sempre riservata al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sulla adozione di ogni provvedimento». L'attività giurisdizionale rientra tra quelle che, se interessate dall'utilizzo di sistemi di IA, può comportare un rischio alto e, per tale ragione, è elencata nel già menzionato allegato III dell'AIA.

Infine, pare opportuno soffermarsi brevemente anche su quanto stabilito in materia di diritto d'autore. Intervenendo sull'art. 40-*bis* del d.lgs. n.

[53] Decreto legislativo 26 maggio 1997, n. 152, "Attuazione della direttiva 91/533/CEE concernente l'obbligo del datore di lavoro di informare il lavoratore delle condizioni applicabili al contratto o al rapporto di lavoro".

[54] In materia di discriminazioni sul luogo di lavoro derivanti dall'uso di sistemi di intelligenza artificiale, v., per tutte, la discussa ordinanza del Tribunale di Bologna, del 31 dicembre 2020, che ha statuito che il sistema algoritmico di accesso dei c.d. "*rider*" alle fasce di prenotazione delle sessioni di lavoro adottato da Deliveroo, azienda multinazionale operante nel settore delle consegne del cibo a domicilio, era discriminatorio. V. le note di M. Faioli, *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, in *Diritto delle relazioni industriali*, 2021, p. 204 ss.; G. Gaudio, *La CGIL fa breccia nel cuore dell'algoritmo di Deliveroo: è discriminatorio*, in *Rivista italiana di diritto del lavoro*, 2021, p. 188 ss.

[55] V., in tal senso, il considerando n. 9 dell'AIA.

[56] Corsivo aggiunto.

208/2021[57], che attua la direttiva (UE) 2018/1808 relativa alla fornitura di servizi di media audiovisivi, l'art. 23 del ddl ha previsto che «*[q]ualunque contenuto* informativo diffuso da fornitori di servizi audiovisivi e radiofonici tramite *qualsiasi* piattaforma in *qualsiasi* modalità incluso il video *on demand* e lo *streaming* [...] che sia stato, attraverso l'utilizzo di sistemi di intelligenza artificiale, completamente generato ovvero, anche parzialmente, modificato o alterato in modo tale da presentare come reali dati, fatti e informazioni che non lo sono, deve essere reso, a *cura dell'autore o del titolare dei diritti di sfruttamento economico, se diverso dall'autore*, chiaramente visibile e riconoscibile da parte degli utenti [...]»[58]. Il segno di identificazione «deve essere presente sia all'inizio della trasmissione e all'inizio del contenuto, sia alla fine della trasmissione e alla fine del contenuto, nonché ad ogni ripresa del programma a seguito di interruzione pubblicitaria». L'onere di dichiarare se eventuali contenuti video includano contenuti generati, modificati o alterati, anche solo parzialmente, in qualsiasi forma e modo, attraverso l'uso di sistemi di IA «di cui sono a conoscenza o si possa ragionevolmente presumere che siano a conoscenza» spetta anche a tutti i fornitori di piattaforme per la condivisione di video (l'art. 23 del ddl, infatti, è intervenuto anche sull'art. 42, comma 7, del predetto d. lgs., che enuclea le misure di tutela a favore dei fruitori di piattaforme video).

La disposizione *de qua*, come meglio si vedrà *infra*, § 4, è quella che, a ben vedere, pone le maggiori questioni in punto di compatibilità con il diritto dell'Unione europea.

4. *I due (primi ed eventuali) profili di incompatibilità del ddl con il diritto dell'Unione europea*

Con riguardo agli eventuali profili di incompatibilità del ddl con il diritto dell'Unione europea e, in specie, con l'AIA, il considerando n. 3 constata che «[a]lcuni Stati membri hanno già preso in esame l'adozione di regole nazionali» in materia, in un certo senso "ammonendoli": normative nazionali divergenti, infatti, si legge, «possono determinare una frammentazione

[57] Decreto legislativo 8 novembre 2021, n. 208, "Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato".

[58] Corsivi aggiunti.

del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA».

Come accennato, il ddl risulta particolarmente agile, breve, financo "asciutto" e le disposizioni ivi contenute si connotano per essere, nel complesso, piuttosto generiche e vaghe. Da tale latitudine della descrizione normativa è difficile discendano significative problematiche in punto di compatibilità con il diritto UE. D'altronde, è lo stesso ddl, all'art. 22, a prevedere una serie di deleghe al Governo affinché adotti, entro dodici mesi dall'entrata in vigore della legge, uno o più decreti legislativi per l'adeguamento della normativa nazionale all'AIA, ed è probabile che sia su questi decreti attuativi che si "giocherà" la partita della conformità della legislazione nazionale con quella "comunitaria". A ciò si aggiunga il Governo ha trasmesso alla Commissione il testo della misura ai fini dell'instaurazione di un dialogo costruttivo su eventuali profili di incompatibilità, che possono (e potranno) in tal modo essere corretti, anche nell'ottica di prevenire future ed eventuali procedure di infrazione *ex* art. 258 TFUE. Tale trasmissione, come meglio si comprenderà *infra*, in questo §, potrebbe essere opportuna, da un lato, per ossequiare il principio di leale cooperazione *ex* art. 4, par. 3, TUE, ma anche, dall'altro lato, in ragione dell'apparente introduzione, da parte del legislatore nazionale, di (almeno una) c.d. regola tecnica[59] ai sensi della direttiva (UE) 2015/1535, che stabilisce una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione[60]. Qualora, infatti, una normativa interna introduca delle "regole tecniche", per tali intendendosi, per quanto qui rileva, «specificazioni tecniche o altri requisiti o regole relative ai servizi la cui osservanza è obbligatoria, *de jure* o *de facto*, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro o in una parte importante di esso [...]», gli Stati membri

[59] Ai sensi dell'art. 1, par. 1, lett. f), della direttiva (UE) 2015/1535, una «regola tecnica» è «una specificazione tecnica o altro requisito o una regola relativa ai servizi, comprese le disposizioni amministrative che ad esse si applicano, la cui osservanza è obbligatoria, *de jure* o *de facto*, per la commercializzazione, la prestazione di servizi, lo stabilimento di un fornitore di servizi o l'utilizzo degli stessi in uno Stato membro o in una parte importante di esso, nonché, fatte salve quelle di cui all'articolo 7, le disposizioni legislative, regolamentari o amministrative degli Stati membri che vietano la fabbricazione, l'importazione, la commercializzazione o l'utilizzo di un prodotto oppure la prestazione o l'utilizzo di un servizio o lo stabilimento come fornitore di servizi».

[60] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

devono, ai sensi dell'art. 5, par. 1, della direttiva, comunicarlo «immediatamente» alla Commissione[61].

Tornando su tali aspetti nel prosieguo, pare potersi affermare che, nel complesso, e al netto delle considerazioni sulla sua opportunità, su cui v. *infra*, § 5, il ddl non sembra ostacolare l'applicabilità diretta del regolamento. D'altro canto, come si è visto *supra*, § 3, la (quasi) totalità delle norme del ddl concerne settori (come la sicurezza e la difesa nazionale, la sanità, il lavoro, la pubblica amministrazione) che non sono dettagliatamente regolati dal regolamento[62]. Facendo poi riferimento alle disposizioni di questo, sebbene esse non impongano o non consentano espressamente agli Stati membri l'adozione di misure di attuazione né precisino il loro margine di discrezionalità in fase di applicazione, è altresì vero che, come accennato *supra*, § 2, esse, assumendo un carattere assimilabile maggiormente a quello di una direttiva che non a quello di un regolamento, richiedono *de facto* l'adozione di misure di applicazione (come d'altro canto riconosciuto dallo stesso ddl all'art. 22, che, come già accennato, attribuisce la delega al Governo ad adottare «uno o più decreti legislativi per l'adeguamento della normativa nazionale al regolamento del Parlamento europeo e del Consiglio sull'intelligenza artificiale»).

L'obbligo di osservare i principi generali del diritto dell'Unione sembra parimenti rispettato[63], tenuto conto che sin dal principio del ddl, il legislatore italiano stabilisce che le sue disposizioni si interpretano e si applicano conformemente al diritto dell'Unione (*ergo* anche ai suoi principi generali). In generale, il ddl non pare nemmeno dissimulare la natura del regolamento, limitandosi a precisare l'esercizio del (fisiologico e tendenzialmente ampio) margine discrezionale loro conferito dall'AIA[64].

Eppure, sebbene a livello di "sistema" non sembrano emergere particolari problemi di sovrapposizione, conflitto, incompatibilità con l'AIA, è calandosi nel dettaglio delle specifiche disposizioni che sorgono le prime e

[61] Tale norma è, evidentemente, una specificazione dell'art. 4, par. 3, TUE. Il considerando n. 5 della direttiva, in effetti, recita che è «ai sensi dell'articolo 4, paragrafo 3, del trattato sull'Unione europea» che gli Stati membri devono notificare all'UE i progetti nel settore delle regolamentazioni tecniche.

[62] Sul principio per cui finché una normativa nazionale non rientra nell'ambito di applicazione del regolamento che intende attuare, quest'ultimo non può ostare ad essa, v. le conclusioni dell'Avv. gen. Szpunar, dell'11 gennaio 2024, C-662/22 e C-667/22, *Airbnb Ireland*, par. 125.

[63] V., in proposito e per tutte, Corte giust. 12 aprile 2018, C-541/16, *Commissione/ Danimarca*, punti 49 e 50; 15 maggio 2014, C-135/13, *Szatmári Malom*, punto 65.

[64] In questi termini, *ex multis*, v. Corte giust. 7 luglio 2016, C-111/15, *Občina Gorje*, punto 35.

più serie perplessità sulla conformità del ddl.

La prima e più evidente è quella relativa alla disciplina in materia di diritto d'autore. Come già accennato, il ddl, all'art. 23, comma 1, lett. b), dispone che «*qualunque*» contenuto informativo diffuso tramite «*qualsiasi*» piattaforma in «*qualsiasi*» modalità, incluso «*il video* on demand *e lo* streaming»[65] che siano stati generati, modificati, alterati anche parzialmente da intelligenza artificiale, deve essere reso, «a cura dell'autore o del titolare dei diritti di sfruttamento economico, chiaramente visibile e riconoscibile, sia all'inizio che alla fine della trasmissione del contenuto». Il medesimo articolo, alla lettera c), emendando l'art. 42, comma 7, del già menzionato d.lgs. n. 208/2021, impone che i fornitori di piattaforme per la condivisione di video siano tenuti ad avere una specifica funzione che consenta agli utenti che caricano contenuti video generati dagli utenti stessi di dichiarare se tali contenuti video contengono contenuti generati, modificati o alterati attraverso l'intelligenza artificiale e non solo di cui siano effettivamente a conoscenza, ma anche di cui siano «ragionevolmente a conoscenza».

Il ddl, con tali disposizioni, pone invero limiti molto più solidi e stringenti di quanto non faccia il regolamento, che, all'opposto, si mantiene su termini decisamente più generici e flessibili. In effetti, l'unica disposizione dettata in materia, l'art. 53, comma 1, lett. c), che enuclea gli obblighi dei fornitori di modelli di IA per finalità generali, impone meramente (e genericamente) che i predetti fornitori «attu[i]no una politica volta ad adempiere alla normativa dell'Unione in materia di diritto d'autore», in particolare per individuare e rispettare le eventuali riserve dei diritti espresse dai loro titolari. Ciò significa, in altri termini, che i fornitori devono (genericamente) disporre di politiche atte a garantire il rispetto del diritto d'autore nel corso della formazione dei loro modelli. A ciò si aggiunga che il considerando n. 109, da leggersi in concerto con l'art. 53, afferma che il rispetto degli obblighi applicabili ai fornitori di modelli di IA per finalità generali «dovrebbe essere *commisurato* e *proporzionato* al *tipo* di fornitore del modello, escludendo la necessità di adempimento per le *persone* che sviluppano o utilizzano modelli per finalità non professionali o di ricerca scientifica, le quali dovrebbero tuttavia essere incoraggiate a rispettare volontariamente tali obblighi» e, certo, sempre «fatta salva la normativa UE in materia di diritto d'autore, «il rispetto di tali obblighi dovrebbe *tenere debitamente conto delle dimensioni* del fornitore e consentire modalità semplificate di adempimento per le PMI, comprese le *start-up*, che *non dovrebbero comportare costi*

[65] Corsivi aggiunti.

eccessivi né scoraggiare l'uso di tali modelli»[66].

Ora, il ddl, imponendo obblighi piuttosto stringenti non solo ai fornitori dei modelli, ma a qualsiasi piattaforma che trasmetta qualsivoglia tipo di contenuto, pare eccedere nella regolamentazione, imponendo oneri ulteriori rispetto a quanto richiesto dal diritto UE. Il ddl, da un lato, introduce dei meccanismi operativi più gravosi e complessi rispetto a quanto espressamente richiesto dal regolamento, che impone esclusivamente la predisposizione di "*policy*" a tutela del diritto d'autore, e, dall'altro lato, pare altresì estendere l'ambito soggettivo di applicazione delle regole UE, dal momento che, come accennato, i suoi destinatari non sembrano essere i soli fornitori di modelli di IA per finalità generali (ad esempio ChatGPT), ma qualsiasi piattaforma, sia essa *web*, televisiva, audiovisiva, di piccole o di grandi dimensioni. Il ddl, in altri termini, sembra aver posto in essere, perlomeno *prima facie*, del "*gold-plating*" attivo[67], verosimilmente illegittimo. Infatti, affinché il *gold-plating* sia legittimo è a monte necessario che il livello di armonizzazione richiesto dall'atto di derivazione "comunitaria" sia minimo[68]. Viceversa, qualora venga imposta un'armonizzazione massima, non potendo gli Stati membri discostarsi da quanto previsto dall'atto UE, ogni eventuale sovraregolamentazione è verosimilmente fonte di una violazione del diritto dell'Unione, in quanto tale suscettibile di essere contestata con una procedura di infrazione[69].

Ora, è chiaro che l'uso del regolamento da parte del legislatore UE indurrebbe a ritenere che il grado di armonizzazione richiesto dall'AIA sia, a ben vedere, massimo, con la conseguenza che la suddetta disposizione costituirebbe *gold-plating* illegittimo. Eppure, come si è visto, il tenore del regolamento non è eccessivamente prescrittivo e svariati spazi d'azione sono lasciati agli Stati membri, con ciò potendosi affermare che il grado di armonizzazione, se non propriamente minimo, non sia in senso stretto nemmeno massimo e, quindi, l'illegittimità dell'art. 23 del ddl sarebbe tutta da verificare. Non può che condividersi, quindi, l'osservazione dottrinale per

[66] Corsivi aggiunti.

[67] Con *gold-plating* attivo si intende la circostanza per cui il legislatore nazionale *aggiunge* requisiti ulteriori e diversi rispetto a quelli previsti nella disciplina UE rilevante. Con *gold-plating* passivo, invece, si intende l'ipotesi in cui il legislatore, non abrogando delle disposizioni nazionali preesistenti alla normativa UE, *mantiene* dei requisiti ulteriori e diversi. In argomento sia concesso rinviare a C. BURELLI, *op. cit.*, p. 632.

[68] *Ibidem*, p. 635.

[69] V., in questo senso, G. RIVELLINI, *Il divieto di gold-plating e il problema della sua giustiziabilità in Italia*, in *Rivista trimestrale di diritto pubblico*, 2021, p. 815 ss., spec. p. 829.

cui «complessivamente inteso, l'approccio del legislatore [UE] [...] pare voler superare la rigida distinzione tra armonizzazione minima e massima in favore di un approccio maggiormente pragmatico, probabilmente dettato dall'ambito specifico oggetto di intervento normativo»[70].

Il rischio, comunque e in ogni caso, è che si generi incertezza giuridica, in specie sulla corretta interpretazione e applicazione della norma "comunitaria", con conseguente disomogeneità nell'applicazione della stessa tra i vari Stati membri. L'imposizione di oneri (più) stringenti a tutti gli operatori italiani, quindi anche alle piccole piattaforme, può comportare, a prescindere dalle riflessioni sulla natura giuridica della disposizione e sul grado di armonizzazione che impone l'AIA, delle discriminazioni tra piccole piattaforme (italiane) e grandi piattaforme (europee e internazionali) che non sono sottoposte ai limiti italiani.

Inoltre, come accennato, occorre chiedersi se tale disposizione possa rappresentare una "regola tecnica" ai sensi della già menzionata direttiva (UE) 2015/1535 (v. *supra*, in questo §). In effetti, imponendo dei requisiti (ulteriori)[71] per la commercializzazione e l'utilizzo dei «contenut[i] informativ[i]» di cui all'art. 23 del ddl, il legislatore nazionale sembra effettivamente aver introdotto una nuova regola tecnica. Naturalmente, ciò diventerebbe problematico nella misura in cui la disposizione, in forza dell'art. 5, par. 1, comma 6, della direttiva, creasse eventualmente ostacoli alla libera circolazione dei servizi nell'ambito del mercato interno. In ogni caso, se, come anticipato, l'Italia avesse comunicato il progetto di norma alla Commissione, cosa che è presumibile abbia fatto, e qualora la Commissione avesse espresso perplessità sulla sua conformità nel parere circostanziato che è tenuta a trasmettere allo Stato ai sensi dell'art. 6, par. 2, comma 2, della direttiva, è difficile immaginare che l'Italia mantenga la norma invariata. Il carattere estremamente tecnico di siffatte disposizioni, che non possiedono un pregnante valore politico, infatti, in uno con l'obbligo informativo (*ergo*, meramente procedurale) che gli Stati sono tenuti ad assolvere *prima* della formale adozione della norma, che ha evidenti finalità preventive, induce a ritenere che gli Stati membri siano tendenzialmente rispettosi degli obblighi deri-

[70] Così M. INGLESE, *op.cit.*, p. 16.

[71] Ai sensi dell'art. 1, par. 1, lett. d), della direttiva (UE) 2015/1535, con «altro requisito» si intende «un requisito diverso da una specificazione tecnica, prescritto per un prodotto per motivi di tutela, in particolare dei consumatori o dell'ambiente, e concernente il suo ciclo di vita dopo la commercializzazione, quali le sue condizioni di utilizzazione, di riciclaggio, di reimpiego o di eliminazione, qualora tali condizioni possano influenzare in modo significativo la composizione o la natura del prodotto o la sua commercializzazione».

vanti dalla direttiva *de qua*. Ciò pare corroborato dal fatto che, all'oggi, non esistono sentenze *ex* art. 258 TFUE (e tanto meno *ex* art. 260 TFUE) per violazione della direttiva[72].

Un'altra norma che fa sorgere delle perplessità in termini di compatibilità con l'AIA è l'art. 2, comma 1, lett. c), del ddl che definisce i «modelli di intelligenza artificiale». La definizione posta dal ddl pare in effetti ora più ristretta, ora più estesa di quella offerta dal regolamento. Quest'ultimo, infatti, prevede che i modelli, «*anche* laddove sia[no] addestrat[i] con grandi quantità di dati utilizzando l'autosupervisione su larga scala»[73], siano caratterizzati da «una generalità significativa [di dati] e sia[no] in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui i modell[i] [sono] immess[i] sul mercato, e che [possono] essere integrat[i] in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato». Il regolamento, inoltre, introduce il concetto di modello di IA per finalità generali con rischio sistemico, che comporta, cioè, un impatto significativo sul mercato dell'Unione «a causa della sua portata» o per gli effetti negativi che ha (o ragionevolmente potrebbe avere) «sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso». Nel ddl i modelli di IA sono, invece, quelli che identificano «strutture ricorrenti attraverso l'uso di collezioni di

[72] È attualmente pendente un ricorso per inadempimento contro l'Ungheria, proposto in data 23 febbraio 2024, causa C-144/24, per violazione dell'obbligo *ex* art. 5, par. 1, della direttiva, cioè l'obbligo di comunicare il progetto di norme tecniche alla Commissione, e per la conseguente violazione dell'art. 49 TFUE. Con riferimento all'Italia, la Corte di giustizia si è pronunciata nell'ambito di un rinvio pregiudiziale stabilendo che la direttiva in materia di regole tecniche osta all'adozione di una normativa nazionale «che vieti la commercializzazione di sacchi monouso fabbricati a partire da materiali non biodegradabili e non compostabili, ma rispondenti [ad] altri requisiti stabiliti nella direttiva [...] sugli imballaggi [...] quando tale normativa sia stata comunicata alla Commissione europea solo qualche giorno prima della sua adozione e pubblicazione». Si era posto, quindi, un tema di (intempestiva) comunicazione alla Commissione della misura nazionale, ma anche un problema di *gold-plating:* l'Italia, infatti, stabilendo il divieto di commercializzazione di sacchi monouso non biodegradabili, ma comunque rispondenti ad altri *standard* europei, aveva imposto una normativa più stringente illegittima, eventualmente giustificabile solo nella misura in cui avesse risposto a finalità di tutela dell'ambiente e sempre che fossero soddisfatte le condizioni di cui all'art. 114, parr. 5 e 6, TFUE. Tali paragrafi stabiliscono, rispettivamente, un obbligo di notifica alla Commissione delle misure *de quibus* e il dovere della Commissione di verificare se esse costituiscano o meno uno strumento di discriminazione arbitraria o una restrizione dissimulata nel commercio tra gli Stati membri. V. Corte giust. 21 dicembre 2023, C-86/22, *Papier Mettler Italia*.

[73] Corsivo aggiunto.

dati, che hanno la capacità di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni».

La differenza più evidente è che la nozione posta dal regolamento comprende *anche* l'ipotesi in cui la supervisione sia effettuata autonomamente, quindi dallo stesso modello tramite un sistema di "intelligenza artificiale", mentre tale circostanza non è inclusa nella definizione del testo italiano, che induce quindi a ritenere che, nel sistema nazionale, la funzione di supervisionare sul modello possa essere attribuita solo all'uomo, escludendosi così l'autosupervisione. La definizione "comunitaria", inoltre, esclude espressamente dal suo campo di applicazione i modelli di IA utilizzati prima della loro immissione sul mercato per soli scopi di ricerca, sviluppo e prototipazione (esclusione che non pregiudica, naturalmente, l'obbligo di conformarsi al regolamento quando, terminate tali attività, il modello sia immesso sul mercato, come chiarisce il considerando n. 97). Il fatto, peraltro, che tale esplicita "dispensa" non sia prevista dal ddl potrebbe far intendere l'inclusione di tali attività nella nozione di modello di IA.

Tale difformità tra le definizioni di modelli di intelligenza artificiale contenute nell'AIA e nel ddl potrebbe, in potenza, generare problemi in punto di uniforme applicazione del regolamento e il perseguimento degli obiettivi da esso perseguiti.

5. *Qualche riflessione conclusiva sull'inopportunità (e l'intempestività) della misura nazionale*

Come ricordato in apertura del lavoro, l'approvazione da parte del Consiglio dei ministri del ddl in materia di intelligenza artificiale, oltre a stimolare delle domande sull'eventuale compatibilità delle sue disposizioni con il diritto dell'Unione europea, consente anche di interrogarsi sull'opportunità *strico sensu* della sua adozione. Come anticipato, infatti, il legislatore italiano – presumibilmente per alimentare il consenso elettorale attraverso la regolazione di un settore, qual è quello dell'intelligenza artificiale, che gode di una certa risonanza mediatica – ha deciso di "anticipare" il legislatore dell'Unione. L'AIA, infatti, pur essendo già entrato in vigore, non inizierà ad applicarsi prima del 2 agosto 2026[74], verosimilmente dopo la pubblicazione in Gazzetta ufficiale della legge nazionale – considerato che il tempo medio di approvazione dei ddl di iniziativa governativa di natura ordinaria con de-

[74] Salvo le eccezioni di cui si è dato conto *supra*, § 1, nota 19.

leghe al Governo, com'è nel caso di specie, è di ottantasette giorni al Senato e di novantanove giorni alla Camera[75] (per un totale, quindi, di centoottantasei giorni, circa sei mesi).

La questione, così posta, assume una certa rilevanza esclusivamente in termini di opportunità politica. Peraltro, la celerità del legislatore italiano rischia, in prospettiva, di essere (ulteriormente) problematica anche in termini di conformità con il diritto dell'Unione. Posto che, forse, sarebbe stato preferibile che il Governo presentasse alle Camere, unitamente al suo disegno di legge, anche un'analisi di impatto della regolamentazione (la c.d. "AIR"[76]), affinché vi fosse una valutazione anticipata degli effetti dell'intervento normativo *de quo* e, quindi, anche una valutazione preventiva delle aree e delle fattispecie che richiedevano effettivamente l'adozione di una normativa nazionale, ciò che più preoccupa è il futuro rapporto tra la legge nazionale (e i suoi decreti attuativi) e gli atti esecutivi e gli atti delegati che adotterà la Commissione europea, su cui, come accennato *supra*, § 2, il regolamento fa molto affidamento per favorire l'efficacia e il perseguimento degli obiettivi dell'AIA. Come rilevato in dottrina, tale «posizione dominante»[77] attribuita alla Commissione «altro non è che la prosecuzione di un approccio in corso di sperimentazione con il DSA e DMA e che prende le distanze dai meccanismi di *enforcement* a trazione nazionale che contrassegnano il GDPR»[78]. In altri termini, se il modello adottato dal regolamento generale

[75] L'informazione statistica è contenuta *online* sul sito del Senato al seguente *link*: www.senato.it/leg/13/BGT/Schede/Statistiche/Stato/TempiApprovazioneDDL.html.

[76] L'AIR è disciplinata dall'art. 14 della legge 28 novembre 2005, n. 246. Ai sensi del comma 1 dell'articolo, l'AIR è la «[...] valutazione preventiva degli effetti di ipotesi di intervento normativo ricadenti sulle attività dei cittadini e delle imprese e sull'organizzazione e sul funzionamento delle pubbliche amministrazioni, mediante comparazione di opzioni alternative». La disciplina sull'AIR è completata dal decreto del Presidente del Consiglio dei Ministri, del 15 settembre 2017, n. 169, e dalla direttiva del Presidente del Consiglio dei ministri, del 16 febbraio 2018. In dottrina, v., per tutti, B. G. Mattarella, *Analisi di impatto della regolazione e motivazione del provvedimento amministrativo*, in *Osservatorio AIR*, 2010, p. 4 ss.; G. Mazzantini, N. Rangone (a cura di), *L'analisi di impatto e gli altri strumenti per la qualità della regolazione*, in *Osservatorio AIR*, 2019, e i contributi ivi contenuti.

[77] Così F. Ferri, *op. cit.*, p. 17.

[78] *Ibidem*, p. 18. Per un'analisi critica sull'impatto e la portata delle disposizioni del regolamento sui servizi digitali e del regolamento sui mercati digitali, v. B. Kis Kelemen, B. Hohmann, *Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU*, in *Croatian Yearbook of European Law and Policy*, 2023, p. 225 ss. Precedentemente, con toni maggiormente favorevoli, v. D. Fasquelle, E. Inacio, *DMA/DSA : une nouvelle et importante étape dans la régulation européenne des acteurs du numérique*, in *Europe*, 2021, p. 4 ss. In generale, sulla

sulla protezione dei dati (di *enforcement*, di *governance*, ma di applicazione in generale) era a carattere fortemente decentralizzato[79], l'AIA – al pari, in una certa misura, dei c.d. DSA[80] e DMA[81] – ha adottato un modello a carattere (maggiormente) centralizzato, con l'attribuzione, appunto, di ampi poteri alla Commissione. Questo, naturalmente, non pregiudica le competenze delle autorità di vigilanza indipendenti nazionali deputate a monitorare la corretta applicazione e attuazione del regolamento, la cui istituzione è richiesta dall'AIA (v. il considerando n. 153 e l'art. 70), come pure non è incoerente con il largo campo d'azione riservato agli Stati membri e spinge quindi a chiedersi se non sarebbe stato comunque opportuno, per il legislatore nazionale, attendere non solo la pubblicazione effettiva dell'AIA, ma anche l'adozione degli atti delegati e di esecuzione della Commissione che, ancora una volta, potrebbero smentire quanto (intempestivamente) stabilito e regolato dal legislatore nazionale, determinandosi, sì, a quel punto, una potenziale situazione di difformità con il diritto UE.

In ogni caso, per il momento, si può ragione se un siffatto intervento normativo nazionale possa comunque «dissimulare ai singoli»[82] il diritto "comunitario" direttamente applicabile, così come se esso «snaturi di fronte agli amministrati il diritto proprio dell'Unione e gli effetti che ne derivano»[83] e, si è visto, probabilmente ciò non avviene. Occorre però chiedersi se non sia comunque un atto che «deformi»[84], in un certo qual modo, il diritto UE, creando un'inopportuna sovrapposizione con esso e una conseguente problematica incertezza del diritto.

strategia per il completamento del mercato unico digitale, v. M. INGLESE, *op. cit.*, spec. p. 6 ss.

[79] Lo evidenziano, *inter alia*, F. BRITO BASTOS, P. PALKA, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, in *European Competition Law Review*, 2023, p. 485 ss. Su alcune delle problematiche che derivano da tale impostazione, specialmente nei casi che presentano natura transfrontaliera, v. G. GENTILE, O. LYNSKEY, *Deficient by Design? The Transnational Enforcement of the GDPR*, in *International and Comparative Law Quarterly*, 2022, p. 799 ss.

[80] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

[81] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828.

[82] In questi termini, Corte giust. 25 novembre 2021, C-372/20, *Finanzamt Österreich* (Allocations familiales pour coopérant), punto 45.

[83] Così Corte giust. 31 gennaio 1978, 94/77, *Zerbone*, punto 26.

[84] Per dirla con R. LUZZATTO, *op. cit.*, p. 1288.

Abstract (ita)

Il contributo svolge un raffronto tra il regolamento UE che stabilisce regole armonizzate sull'intelligenza artificiale e il ddl italiano per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale, esaminando, in specie, le "ricadute" istituzionali e politiche dell'atto nazionale. A questo fine, il lavoro ricostruisce brevemente i caratteri fondamentali di tali provvedimenti, dando particolare evidenza alle disposizioni relative alla loro applicazione. Dopodiché, enuclea i primi ed eventuali profili di incompatibilità del ddl italiano con il diritto dell'Unione europea, per svolgere, infine, brevi riflessioni sull'inopportunità (e l'intempestività) della misura nazionale.

Abstract (eng)

This contribution compares the Artificial Intelligence Act with the Italian draft law on the artificial intelligence, analyzing, in particular, the institutional and political consequences of the national act. To this end, the paper shortly traces the measures' features, highlighting the provisions relating to their application. Then, it illustrates the first and possible profiles of incompatibility of the Italian draft law with EU law. Finally, it carries out some reflections on the appropriateness and timeliness of the national measure.