Università degli Studi del Molise

III EDIZIONE

DIZIONARIO SISTEMATICO DEL DIRITTO DELLA CONCORRENZA ITALIANO E DELL'UNIONE EUROPEA

Regolamentazione UE

a cura di
Lorenzo Federico Pace

Edizioni Efesto

L'arte del buono e del giusto

Università
degli Studi
del Molise

DIZIONARIO SISTEMATICO DEL DIRITTO DELLA CONCORRENZA ITALIANO E DELL'UNIONE EUROPEA

Regolamentazione UE – vol. 3

III Edizione

a cura di
Lorenzo Federico Pace

EdizioniEfesto

DIZIONARIO SISTEMATICO DEL DIRITTO DELLA CONCORRENZA ITALIANO E DELL'UNIONE EUROPEA

III Edizione – Vol. III

Efesto Libri SRLS - Via Corrado Segre, 11 (Roma)
06.5593548 - info@edizioniefesto.it
www.edizioniefesto.it

Collana: *L'arte del buono e del giusto*

Curatore: *Lorenzo Federico Pace*

ISBN 978-88-3381-791-0
gennaio 2026

Impaginazione e stampa:
Libreria Efesto | **edizioniefesto.it**

DIZIONARIO SISTEMATICO DEL DIRITTO DELLA CONCORRENZA ITALIANO E DELL'UNIONE EUROPEA

Vol. 3 - Indice

VOLUME 3

IL REGOLAMENTO SULL'INTELLIGENZA ARTIFICIALE (*AI ACT*)

Sommario: **I.** Alle origini della riforma. – I.1. L'evoluzione della strategia sull'IA nel quadro della transizione digitale dell'Unione. – I.2. Punti di contatto con il DSA e il DMA. – **II.** *AI Act* e approccio al rischio. – II.1. I paradigmi del rischio alto e del rischio sistemico. – II.2. Principali limiti e obblighi in funzione delle categorie di rischio. – **III.** *AI Act* e profili innovativi in tema di *governance*. – III.1. Livello nazionale: natura, tipologia e funzioni primarie delle autorità indipendenti. – III.2. Livello sovranazionale: organi competenti e influenza della Commissione europea. – **IV.** Attuazione dell'*AI Act* ed esigenze di leale cooperazione. – IV.1. Monitoraggio interno e dimensione "orizzontale" della leale cooperazione. – IV.2. Monitoraggio multilivello e dimensione "verticale" della leale cooperazione.

I. Alle origini della riforma

Il settore dell'intelligenza artificiale (IA) rappresenta indubbiamente una delle frontiere più estreme del processo di integrazione europea. Ad oggi, esso risulta disciplinato a livello sovranazionale in particolare dal Regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'intelligenza artificiale[1] (di seguito, Regolamento sull'IA o *AI Act*), applicabile salve alcune eccezioni dal 2 agosto 2026.

La scelta dell'Unione di introdurre una disciplina *ad hoc* per l'IA ha destato molto scalpore e arricchisce il sistema UE di regole nel campo del digitale e delle nuove tecnologie, nel tentativo di coniugare due priorità di carattere generale: colmare le lacune tecnologiche che separano l'Unione dalle principali economie mondiali e difendere l'assetto assiologico sovranazionale in un contesto geopolitico sempre più "incandescente". In sintesi, il Regolamento sull'IA è il frutto degli intrecci tra direttrici che muovono da due paradigmi sempre più sovrapposti: lo sviluppo del mercato interno, oggi nella sua accezione digitale, e la tutela dei diritti fondamentali, ora più che mai sotto l'egida dei valori comuni e fondanti *ex* art. 2 TUE[2].

Come noto, il Regolamento sull'IA costituisce uno dei primi esempi a livello globale di intervento normativo in *subiecta materia*; tuttavia, è bene ricordare sin da ora che il processo di riforma culminato con l'adozione di tale atto è iniziato tempo addietro. È, infatti, guardando dapprima ai lavori preparatori che si possono cogliere alcuni elementi di contesto, per certi versi dotati di rilevanza sostanziale. Dalle fasi della gestazione dell'*AI Act* emergo-

[1] Reg. (UE) n. 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), in G.U.U.E L 12 luglio 2024, p. 1.

[2] Ai sensi dell'art. 2 TUE, "L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini".

no in maniera paradigmatica, a seconda del momento, tanto le sinergie quanto le tensioni tra le istituzioni coinvolte nella procedura legislativa ordinaria. In altre parole, si colgono con chiarezza le dinamiche tra quei centri di potere che rappresentano soggetti (e interessi) diversi nell'ambito dell'ordinamento giuridico dell'Unione europea; un ordinamento che, come illustrato più di sessant'anni fa dalla Corte di giustizia nella sentenza *Van Gend en Loos*[3], è un *unicum* nel panorama della soggettività internazionale anche in virtù delle anime che lo compongono.

I.1. L'evoluzione della strategia sull'IA nel quadro della transizione digitale dell'Unione

A partire all'incirca dal 2018 il tema dell'IA ha iniziato a campeggiare nella narrativa delle istituzioni politiche dell'Unione. Se Consiglio europeo e Consiglio dell'Unione lo hanno accennato in misura più sfumata e il Parlamento europeo lo ha ricondotto principalmente a prerogative di tutela dei diritti fondamentali e della sicurezza degli individui, la Commissione europea lo ha affrontato con un approccio sempre più organico e pervasivo. Al riguardo, si può suddividere in due fasi l'intero arco temporale dei lavori preparatori.

La prima fase, orientata dalla Commissione "Juncker" quando ormai era giunta a fine mandato, è servita più che altro per inserire l'IA nell'agenda politico-programmatica dell'Unione. Si segnala una prima strategia, dell'aprile 2018, intitolata "L'intelligenza artificiale per l'Europa"[4], nella quale si esortava espressamente all'accettazione del cambiamento e veniva spiegato come l'IA non fosse fantascienza, bensì un fenomeno già in evoluzione ("come il motore a vapore o l'elettricità nel passato, l'IA sta trasformando il nostro mondo, la nostra società e la nostra industria"). Alla fine di quell'anno la Commissione pubblicava un Piano coordinato sull'intelligenza artificiale, vale a dire un una serie di azioni comuni per aumentare gli investimenti e la cooperazione, specie tramite gli scambi di buone pratiche. Il fulcro della programmazione strategica della Commissione si spostava quindi sull'approccio antropocentrico all'IA, cruciale anche per creare fiducia nella transizione: nella prima metà del 2019 veniva rilasciata un'apposita comunicazione[5] e – cosa ancora più importante – si assisteva alla pubblicazione degli "Orientamenti etici per un'IA affidabile"[6], redatti da un gruppo di esperti indipendenti di alto livello nominato proprio dalla Commissione. In sintesi, questa prima fase si è fermata all'anticamera delle attività funzionali all'elaborazione dell'iniziativa legislativa e si è contraddistinta per una spiccata enfasi sulla dimensione, – per così dire – "valoriale".

La seconda fase, invece, guidata dalla Commissione "Von der Leyen" insediatasi alla fine del 2019, è stata improntata sin dalle prime battute alla preparazione di una legislazione in materia. Lo si desume anzitutto dal fatto che una delle priorità indentificate da quella Commissione sin dall'inizio, rinominata "Un'Europa pronta per l'era digitale", fosse destinata a raggiungere una sovranità digitale europea. Inoltre, già nel febbraio del 2020 la Commissione aveva pubblicato un libro bianco sull'IA, finalizzato a comprendere se i rischi con-

[3] C. giust. Ce, 5 febbraio 1963, causa 26/62, *Van Gend en Loos*, ECLI:EU:C:1962:42, p. 23.

[4] Comunicazione della Commissione, L'intelligenza artificiale per l'Europa, 25 aprile 2018, COM(2006) 237 final.

[5] Comunicazione della Commissione, Creare fiducia nell'intelligenza artificiale antropocentrica, 8 aprile 2019, COM(2019) 168 final.

[6] Gruppo Indipendente di Esperti ad Alto Livello sull'Intelligenza Artificiale istituito dalla Commissione Europea nel giugno 2018, Orientamenti etici per un'IA affidabile, 8 aprile 2019.

nessi all'evoluzione dell'IA potessero essere fronteggiati adeguatamente tramite le norme all'epoca vigenti oppure, in alternativa, modificando lo stato dell'arte o introducendo una nuova legislazione. In questo tratto di percorso, si intravedeva anche un'attenzione più spiccata alla dimensione di mercato. Tali circostanze sono sintetizzabili attraverso un passaggio indicativo del libro bianco, nel quale si legge: «(u)n solido quadro normativo europeo per un'IA affidabile proteggerà tutti i cittadini europei e contribuirà a creare un mercato interno senza attriti che favorirà l'ulteriore sviluppo e l'adozione dell'IA rafforzando la base industriale dell'Europa nel campo dell'IA».

Si è così giunti all'elaborazione della proposta di Regolamento sull'IA, pubblicata il 21 aprile 2021 dalla Commissione europea[7]. La proposta di Regolamento ha confermato l'approccio di fondo, che peraltro si ritrova anche nella versione definitiva dell'atto licenziato tre anni dopo. Detto approccio può essere riassunto in due punti prioritari.

Il primo punto è la sopravvivenza della doppia anima della riforma, destinata quindi ad essere il frutto di un compromesso tra esigenze di non frammentazione del mercato interno e delicati equilibri di tutela dei diritti fondamentali e dei valori. La Commissione ha optato per una doppia base giuridica: da un lato, l'art. 114 TFUE, inerente alle misure per il ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno; dall'altro l'art. 16 TFUE, riguardante la tutela dei dati personali. Ora, è vero che il centro di gravità è sicuramente l'art. 114 TFUE, mentre l'art. 16 TFUE è per lo più accessorio. Tuttavia, già nel testo della proposta era possibile scorgere una quantità assai elevata di riferimenti a molteplici diritti fondamentali, nonché un collegamento diretto tra la Carta (più i valori) e la qualificazione in termini di legittimità o meno di condotte di soggetti privati.

Secondariamente, e proprio in virtù della scelta di incidere direttamente sulla sfera giuridica dei singoli attraverso un Regolamento, un tratto caratteristico dell'*iter* è stata la ricerca di una armonizzazione a geometria variabile. Si è stabilito di definire 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 nell'Unione. Eppure, sin dalle valutazioni riportate nello *staff working document* di accompagnamento alla proposta[8], era possibile comprendere che la via da intraprendere avrebbe dovuto essere quella di un unico sistema composto da regimi distinti. Sul piano della tecnica legislativa, ci si riferisce a un'alternanza tra limiti stringenti, obblighi relativamente prescrittivi e traiettorie affidate in buona parte al volontarismo dei soggetti interessati. Circa le fasi di attuazione ed esecuzione, si allude a un insieme di poteri più o meno intenso degli organi nazionali o sovranazionali. I criteri di fondo per stabilire il regime di volta in volta applicabile sono essenzialmente la tipologia e il grado del rischio da affrontare, tenendo presente che tale valutazione è stata in larga misura "centralizzata" a monte, ovverosia dalla Commissione (nella proposta) e da Parlamento europeo e Consiglio (nell'atto

[7] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final.

[8] 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 final.

legislativo): la portata dei vincoli dettati dal Regolamento dipende dunque dalla sussistenza di un rischio inaccettabile, alto, limitato, oppure minimo.

Al netto di queste considerazioni di ordine generale, il testo del Regolamento pubblicato nella Gazzetta ufficiale dell'Unione presenta molte differenze rispetto alla proposta. La circostanza non è sorprendente, se si pensa alla complessità della procedura legislativa ordinaria e alla difficoltà di "fotografare" all'interno di uno strumento di diritto positivo una materia come l'IA, a lungo quasi inimmaginabile dal punto di vista cognitivo e ad oggi comunque in continuo divenire.

Di per sé, l'*AI Act* è un Regolamento poderoso, comprensivo di 180 "considerando", 13 capi, 113 articoli e 13 allegati, dunque nettamente più lungo della proposta. Enuncia numerose definizioni, a cominciare quella di "sistema di IA", allo scopo di favorire l'emersione di concetti unitari, anche se è pacifico che riguardo alla declinazione di alcuni di essi gli Stati membri manterranno un certo margine di manovra. Si precisa altresì che il campo di applicazione non si estende ad alcune aree particolarmente sensibili o strategiche: ad esempio, laddove i sistemi di IA siano collegati a scopi militari, di difesa o sicurezza nazionale, di ricerca e sviluppo scientifico. Tra le altre cose, il Regolamento non incide sulle pratiche vietate dal diritto UE, tra cui quelle coperte dalla normativa in tema di concorrenza.

Nel complesso, l'architettura dell'*AI Act* si regge su un fitto agglomerato di disposizioni costruite attorno ai seguenti punti chiave: vietare le pratiche di IA che comportano rischi inaccettabili; individuare le applicazioni ad alto rischio, stabilire i relativi requisiti e gli obblighi specifici per gli operatori e i fornitori; introdurre una disciplina specifica per i modelli di IA con finalità generali (modelli GPAI), inclusi quelli con rischio sistemico; delineare misure a sostegno dell'innovazione, con particolare riferimento agli spazi di sperimentazione normativa; istituire un quadro di governance a più strati e un sistema di monitoraggio per interventi successivi all'immissione sul mercato.

I.2. Punti di contatto con il DSA e il DMA

Il Regolamento (UE) 2024/1689 si inserisce in un contesto normativo particolarmente fluido, una rete a più nodi che le istituzioni politiche dell'Unione hanno iniziato a tessere – non certo senza fatica e tensioni – da circa un decennio, allorché apparve evidente che il diritto UE avrebbe dovuto essere utilizzato per dare corpo a una vera e propria rivoluzione digitale europea. Molti sono i punti di contatto tra *AI Act* e normative generali o settoriali che si collocano lungo questa direttrice; ma tali intrecci non sorprendono, specie alla luce dell'attitudine di questo Regolamento a espandersi verso ambiti materiali di vario tipo.

Al di là dei fisiologici collegamenti con il Regolamento generale sulla protezione dei dati personali (GDPR)[9] e con atti successivi che l'Unione ha adottato per attuare la strategia europea in materia di dati, l'*AI Act* costituisce un tassello del mosaico rappresentato dal pacchetto sui servizi digitali, entrando dunque in correlazione con i Regolamenti sui servizi e i mercati digitali del 2022 (DSA e DMA)[10]: nel loro insieme,

[9] Reg. (UE) n. 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 G.U.U.E L 119, 4 maggio 2016, p. 1.

[10] Reg. (UE) n. 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 (Regolamento sui servizi digitali), in G.U.U.E L 277, 27 otto-

queste misure costituiscono effettivamente un disegno unitario. D'altronde, il fine del DSA è «contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta (…) siano tutelati in modo effettivo» (art. 1 DSA): allo scopo, questa misura impone obblighi con particolare riferimento a piattaforme *online* e motori di ricerca *online*, soprattutto se di dimensioni molto grandi[11]. Con il DMA, invece, si è inteso «contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (…) siano equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali» (art. 1, DMA)[12].

Ebbene, le tre misure in analisi affrontano rischi parzialmente sovrapponibili, in particolare perché si prefiggono di limitare l'impatto potenzialmente negativo di operatori che detengono una *leadership* in campo tecnologico e che possono sviluppare e utilizzare sistemi e modelli altamente condizionanti per il nucleo attorno al quale si evolve il processo di integrazione europea. Tutti questi atti, non a caso, sono stati ricondotti alla dottrina del "costituzionalismo digitale europeo", oltre che a paradigmi quali la ricerca di una sovranità tecnologica e di una autonomia strategica dell'Unione. A questo riguardo, uno spazio di intersezione tra DSA, DMA e *AI Act* è da rinvenirsi nell'attenzione riservata a grandi piattaforme di IA capaci di penetrare in maniera incisiva e capillare nel mercato interno.

Ciò ha ricadute anche nel diritto UE in materia di concorrenza. Atteso che certi operatori sono in grado di avvalersi dell'IA persino per realizzare condotte anticoncorrenziali, l'*AI Act* a tratti completa lo strumentario con cui l'Unione concretizza i divieti sanciti dagli artt. 101 e 102 TFUE. Ad ogni modo, il Regolamento sull'IA non incide sulle pratiche vietate dal diritto dell'Unione, comprese quelle disciplinate

bre 2022, p. 1; Reg. (UE) n. 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 (Regolamento sui mercati digitali), in G.U.U.E L 265, 12 ottobre 2022, p. 1.

[11] L'art. 3, lett. i) e lett. j), DSA definisce le piattaforme *online* e i motori di ricerca *online* nei seguenti termini: per piattaforma online si intende "un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del (…) Regolamento"; un motore di ricerca *online*, invece, è "un servizio intermediario che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto".

[12] Si precisa che, dal combinato disposto degli artt. 2.1) e 3, par. 1, DMA, un'impresa che fornisce servizi di piattaforma di base è designata come *gatekeeper* "se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro". Le piattaforme online e i motori di ricerca di dimensioni molto grandi sono designati come tali in virtù dei criteri *ex* art. 33 DSA: in particolare, occorre cha abbiano un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni.

dal diritto della concorrenza ("considerando" 45), e all'art. 74, par. 2, stabilisce che le autorità nazionali di vigilanza del mercato, nell'ambito dei loro obblighi di segnalazione a norma dell'art. 34, par. 4, del Regolamento (UE) 2019/1020[13], devono comunicare annualmente alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza qualsiasi informazione "di potenziale interesse per l'applicazione del diritto dell'Unione in materia di concorrenza" che sia stata individuata nel corso delle attività di vigilanza del mercato. Per altro verso, è evidente il tentativo lato UE di includere nel campo di applicazione del DMA anche sistemi e modelli quali l'IA generativa e i *large language models*.

II. *AI act* e approccio al rischio

Il Regolamento 2024/1689 ha il duplice scopo di regolamentare l'utilizzo dell'IA in modo tale da non limitare lo sviluppo tecnologico e, al contempo, fare in modo che il suo utilizzo avvenga nel rispetto dei diritti fondamentali e dei valori europei *ex* art. 2 TUE. In un'ottica di bilanciamento tra sviluppo tecnologico e tutela dei singoli, il Regolamento sull'IA adotta un approccio basato sul rischio, al pari di altri strumenti adottati in ambito digitale e, segnatamente, del GDPR.

II.1. I paradigmi del rischio alto e del rischio sistemico

Il Regolamento vieta l'impiego di quei sistemi di intelligenza artificiale potrebbero compromettere i valori fondanti dell'UE e, nello specifico, la salute, la sicurezza o i diritti fondamentali; un rischio, questo, qualificato come inaccettabile. Tra i sistemi elencati in via esaustiva all'art. 5, vale la pena menzionare quelli di categorizzazione biometrica che utilizzano informazioni sensibili (es. convinzioni politiche, religiose, filosofiche, orientamento sessuale, razza); di raccolta non mirata di immagini facciali da Internet o filmati CCTV per creare database di riconoscimento facciale; di riconoscimento delle emozioni sul posto di lavoro e nelle istituzioni educative; sistemi di *social scoring* basati sul comportamento sociale o sulle caratteristiche personali; sistemi di manipolazione del comportamento umano per aggirare il libero arbitrio; e, infine, sistemi che sfruttano le vulnerabilità delle persone (a causa della loro età, disabilità, situazione sociale o economica).

Per tutti gli altri sistemi, invece, è stata costruita "una piramide del rischio" in cui a diverso livello di rischio corrisponde un'opzione regolatoria, secondo una prospettiva di «precauzione costituzionale». Nello specifico, i sistemi di IA considerati ammissibili sono suddivisi in tre diversi gruppi: sistemi a rischio minimo; sistemi a rischio limitato; e sistemi che comportano un alto rischio.

I sistemi di IA a rischio minimo sono quelli utilizzati per la traduzione automatica, videogiochi o filtri *antispam*; mentre la categoria dei sistemi a rischio limitato include i *software* che impiegano sistemi automatici di intelligenza artificiale (come i *chatbot*) e quelli utilizzati per produrre contenuti audio o video e per identificare le emozioni o rilevare dati biometrici senza l'intento di tracciare l'utilizzatore finale.

I sistemi ad alto rischio sono classificati tenendo in considerazione due parametri: la destinazione d'uso e la loro rilevanza in settori socioeconomici che possono determinare un danno alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia

[13] Reg. (UE) n. 2019/1020 del Parlamento europeo e del Consiglio 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, in G.U.U.E L 169, 25 giugno 2019, p. 1.

e allo Stato di diritto. L'articolazione prevista dall'art. 6 del Regolamento è particolarmente complessa e si avvale dell'allegato III per dettagliare le diverse tipologie di sistemi che ricadono in questa categoria. Tuttavia, non si tratta di una lista esaustiva, dal momento che il Regolamento attribuisce alla Commissione il potere di modificare l'elenco attuale, integrando o rimuovendo i sistemi definiti ad alto rischio sulla base di sviluppi ed esigenze futuri (art. 7).

Nel testo finale dell'*AI Act* sono state altresì inserite norme specifiche per i modelli GPAI, ovvero per quei modelli 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". Essendo addestrati con grandi quantità di dati e con complessità avanzate e avendo capacità e prestazioni ben al di sopra della media, per questi modelli di IA è stata introdotta la classificazione di "rischio sistemico" di cui all'art. 51 del Regolamento.

La scelta di utilizzare una strategia basata sul rischio è a suo modo funzionale ad una opportuna distinzione tra i diversi sistemi di IA e sui modelli su cui questi si basano, garantendo una consapevole valutazione sul loro impatto in termini collettivi. Inoltre, questo tipo di impostazione estende la nozione di "sistema *by design*" anche all'intelligenza artificiale, secondo un approccio precauzionale finalizzato a garantire la sicurezza degli utenti in tutto il ciclo di vita del sistema. Ciononostante, non possono essere sottovalutati i possibili problemi applicativi di questa impostazione vista l'astrattezza e la natura preventiva dell'identificazione del rischio in un contesto, quale quello tecnologico, costantemente in mutazione ed evoluzione.

II.2. Principali limiti e obblighi in funzione delle categorie di rischio

Al fine di garantire una elevata protezione dei singoli già in via preventiva, il Regolamento 2024/1689 prevede, a carico dei fornitori e dei *deployer* [14] dei sistemi di IA, obblighi di natura proporzionale rispetto al loro grado di rischio.

Data la loro natura, per i sistemi a rischio minimo non è prevista alcuna restrizione e viene solamente richiesta l'adesione a codici di condotta e ad un sistema di *accountability* rimesso essenzialmente alla scelta volontaria dei *deployer.* I sistemi a rischio limitato sono sottoposti a obblighi di mera trasparenza e segnalazione in modo tale da garantire che gli individui siano consapevoli che stanno interagendo con una macchina e non con un essere umano. Tenuto conto della delicatezza degli ambiti su cui insistono i sistemi di IA ad alto rischio e il loro potenziale impatto discriminatorio, essi sono invece assoggettati ad una disciplina ben più stringente con obblighi e divieti volti a garantirne la trasparenza, l'affidabilità e il controllo da parte dell'essere umano. In particolare, il Regolamento sull'IA prevede due strumenti applicabili ai sistemi ad alto rischio prima di poter essere introdotti nel mercato dell'Unione: (*i*) una valutazione di conformità e (*ii*) una valutazione d'impatto sui diritti fondamentali.

i) La produzione di una valutazione di conformità (*compliance assessment*) grava sul fornitore dei sistemi di IA secondo modalità analoghe a quelle previste per altri prodotti regolamentati a livello europeo.

[14] Ai sensi dell'art. 3 del reg. 2024/1689, il "*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».

Per poter essere immessi nel mercato, i sistemi e i prodotti di IA appartenenti alla categoria dell'alto rischio dovranno risultare conformi ai requisiti di sicurezza e tutela della salute. Tale valutazione può essere effettuata in tre modi diversi a seconda della natura del sistema interessato.

Nel caso di sistemi di IA utilizzati come componenti di prodotti già valutati in termini di sicurezza (es. dispositivi medici o giocattoli), i requisiti stabiliti nell'*AI Act* saranno integrati nella legislazione in materia di sicurezza settoriale esistente e, dunque, nelle valutazioni di conformità svolte *ex ante* da terze parti. L'obiettivo è quello di evitare la duplicazione degli oneri amministrativi e di mantenere responsabilità distinte, garantendo al contempo una forte coerenza tra i diversi ambiti di regolamentazione.

Invece, i sistemi di IA ad alto rischio utilizzati per il reclutamento, per determinare l'accesso alle istituzioni educative e profilare le persone per le forze dell'ordine sono definiti sistemi autonomi. Quest'ultimi dovranno soddisfare i requisiti stabiliti nell'*AI Act*, che spaziano dalla qualità dei dati utilizzati, alla documentazione tecnica e alla conservazione dei dati, dalla trasparenza alla fornitura di informazioni agli utenti, dalla sorveglianza umana alla robustezza, dall'accuratezza alla cybersecurity; tutti elementi, questi, che devono rispondere ad appositi *standard* di conformità elaborati dai due enti di normazione europea, CEN e CENELEC[15].

I fornitori di sistemi di IA autonomi ad alto rischio hanno due opzioni per condurre valutazioni di conformità. Essi possono effettuare (a) valutazioni di conformità *ex ante* basate sul controllo interno, oppure (b) coinvolgere un revisore esterno (definito "organismo notificato") per valutare il loro sistema di gestione della qualità e la documentazione tecnica. La procedura (a) è un'opzione laddove il sistema di IA autonomo ad alto rischio sia pienamente conforme ai requisiti previsti dal Regolamento. Quando, invece, la conformità sia solo parziale o non esistano ancora norme armonizzate, i fornitori sono obbligati a seguire la procedura (b). A prescindere dalla procedura utilizzata, al termine verrà rilasciata una dichiarazione europea di conformità, emessa dal fornitore e messa a disposizione delle autorità nazionali designate da ciascuno Stato membro, e i sistemi di IA otterranno la marcatura CE e saranno registrati in un'apposita banca dati accessibile al pubblico, per poi essere immessi sul mercato.

A completamento del quadro, occorre sottolineare che l'art. 43 del Regolamento sull'IA prevede un meccanismo di revisione della valutazione di conformità dopo ogni "modifica sostanziale" dei sistemi di IA ad alto rischio, salvo si tratti di sistemi che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio; in questo caso, le variazioni apportate dal fornitore rispetto alla valutazione di conformità originaria non costituiscono una modifica sostanziale.

ii) L'art. 27 del Regolamento stabilisce l'elaborazione di una valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment* o FRIA) a carico dei *deployer* afferenti sia al settore pubblico che a quello privato, essendo questi nella posizione migliore per capire come il sistema di IA ad alto rischio sarà utilizzato concretamente. A motivo, infatti, di una conoscenza più precisa del contesto di utilizzo, i *deployer* sono in grado di identificare potenziali rischi significativi, non previsti nella fase di sviluppo, nei confronti di persone o specifiche categorie di persone, compresi i gruppi emarginati

[15] Commissione europea, Implementing decision C(2023)3215 of 22.5.2023 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.

e vulnerabili. Per questo, la valutazione dovrà essere compiuta prima di mettere in servizio il sistema, valutando, fra gli altri elementi, "le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema", la conformità del sistema con il diritto UE e nazionale in materia di diritti fondamentali e l'impatto ragionevolmente prevedibile sui medesimi. L'operatore dovrà informare l'autorità nazionale di vigilanza e le parti interessate per raccogliere le informazioni pertinenti ritenute necessarie per effettuare la valutazione d'impatto che sarà poi resa disponibile al pubblico.

È rilevante notare che agli operatori di sistemi di intelligenza artificiale ad alto rischio viene permesso di effettuare una valutazione di impatto sui diritti fondamentali congiuntamente a quella sulla protezione dei dati prevista dall'art. 35 del GDPR. Di conseguenza, gli operatori di tali sistemi dovranno eseguire due valutazioni d'impatto: una, più generale, sui i diritti fondamentali (ad esempio il diritto alla salute, il divieto di discriminazione, la tutela dei consumatori e dei gruppi vulnerabili), un'altra, più specifica, focalizzata esclusivamente sulla tutela della riservatezza e dei dati personali. A differenza di quanto accade per le valutazioni di impatto, tuttavia, nel caso del FRIA il Regolamento non precisa nulla circa eventuali revisioni nel caso di potenziali evoluzioni dei sistemi di IA.

A fronte di questi specifici obblighi in capo a fornitori e *deployer* di sistemi di IA ad alto rischio, vale la pena soffermarsi sugli obblighi rispetto ai modelli GPAI che, non essendo propriamente sistemi di IA, sono regolamentati separatamente. Infatti, i fornitori sono soggetti a obblighi distinti che possono essere considerati una versione semplificata degli obblighi per i sistemi di IA. Tra le altre cose, ai sensi dell'art. 53 del Regolamento, devono creare e mantenere la documentazione tecnica, elaborare una politica relativa al rispetto della normativa sul copyright e creare un riepilogo dettagliato del contenuto utilizzato per addestrare il modello GPAI. Quanto, poi, ai modelli GPAI con rischi sistemici, i fornitori hanno ulteriori obblighi *ex* art. 55, tra cui lo svolgimento di valutazioni sui modelli, la valutazione e l'attenuazione dei rischi sistemici, la documentazione e la segnalazione di gravi incidenti, nonché un'adeguata protezione della sicurezza informatica.

Da questa ricostruzione complessiva, pare evidente l'attribuzione di concatenati obblighi di *due diligence* a carico degli operatori privati che, nella fase precedente all'immissione nel mercato dei sistemi di IA, non solo svolgeranno dei test di conformità rispetto agli *standard* stabiliti dagli enti di normazione europei ma saranno altresì chiamati ad effettuare, in via esclusiva, un bilanciamento tra i diritti e gli interessi economici in gioco. Come di seguito illustrato, invece, il Regolamento sull'IA introduce un sistema di *governance* basato su una pluralità di soggetti di natura pubblica, coinvolti nella fase di monitoraggio successiva all'immissione, la messa in servizio e l'uso dei sistemi di IA nel mercato dell'Unione europea.

III. *AI Act* e profili innovativi in tema di governance

Il complessivo sistema di *governance* previsto dall'*AI Act* si articola su un doppio livello: quello nazionale e quello sovranazionale. Il livello nazionale si affida ad un'autorità di notifica e ad un'autorità di vigilanza del mercato operante conformemente al Regolamento (UE) 2019/1020. Invece, il livello sovranazionale – dove la Commissione europea svolge un ruolo determinante – comprende quattro strutture: l'Ufficio per l'IA, di fatto interno alla Commissione; il Consiglio per l'IA,

che comprende rappresentanti degli Stati membri; il Forum consultivo, composto da *stakeholders*; e il Gruppo di esperti scientifici indipendenti. A questi, introdotti specificamente dall'*AI Act*, si aggiunge il Garante europeo per la protezione dei dati personali, cui è affidato il potere di vigilanza rispetto all'utilizzo dei sistemi di IA da parte delle istituzioni europee.

III.1. Livello nazionale: natura, tipologia e funzioni primarie delle autorità indipendenti

L'art. 70 del Regolamento sull'IA 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. Ad ogni modo, come 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». 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. L'attenzione all'imparzialità delle autorità di vigilanza è invece legata 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.

Sul piano operativo, all'art. 74 del Regolamento, il legislatore ha avuto premura di articolare i poteri delle autorità di vigilanza create *ex novo* rinviando esplicitamente al sistema istituito dal Regolamento 2019/1020 e specificando le due funzioni principali.

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.

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. Le autorità potranno quindi chiedere informazioni ai fornitori, compresi quelli di modelli di IA, 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 Regolamento 2019/1020. In alternativa, come stabilito dall'art. 85, «qualsiasi persona fisica o giuridica» che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni dell'*AI Act* potrà presentare all'autorità di vigilanza un reclamo motivato. Questa opportunità 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. Spetterà poi agli Stati membri stabilire le modalità di raccordo con il sistema di tutela giurisdizionale nazionale, una volta designate le autorità competenti.

Qualora le misure correttive 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, par. 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, il Regolamento 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. Tenuto conto di queste soglie, gli Stati membri dovranno stabilire sanzioni efficaci, proporzionate e dissuasive, comprese le sanzioni amministrative, e comunicarle alla Commissione. 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 dall'*AI Act*.

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. 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.

III.2. Livello sovranazionale: organi competenti e influenza della Commissione europea

Ulteriori aspetti innovativi si colgono da un'analisi delle disposizioni riguardanti il livello sovranazionale del sistema di *governance* dell'*AI Act*. Il riferimento va inizialmente al capo VII del Regolamento, ma meritano di essere fatti cenni anche a regole sancite all'interno dei capi IX (in tema di monitoraggio) e XI (sulle sanzioni).

Il dato più evidente, a seguito di una prima lettura dell'atto, è la compresenza di più organi nel sistema di *governance*: nella sezione I del capo VII sono menzionati l'Ufficio per l'IA (art. 64), il Consiglio per l'IA (artt. 65 e 66), il Forum consultivo (art. 67) e il Gruppo di esperti indipendenti (art. 68). Scendendo più nel dettaglio, e guardando anche oltre il Regolamento, si colgono poi vari aspetti interessanti.

Intanto, va detto che solo il Consiglio dell'IA era stato contemplato nella proposta della Commissione, anche se era stato immaginato un "comitato" e comunque in forma diversa dall'organo emerso dalla procedura legislativa. Non va nemmeno dimenticato che l'Ufficio per l'IA, indicato per la prima volta dal Parlamento europeo durante l'*iter*, è stato oggetto di interventi successivi che ne hanno modificato di volta in volta gli aspetti essenziali.

Si sottolinea altresì come la natura di questi organi sia profondamente diversa. L'Ufficio per l'IA è una "funzione" della Commissione, dunque un centro di potere che esprime più o meno direttamente l'essenza "comunitaria" dell'attuazione della normativa. Al contrario, il Consiglio per l'IA è composto di un rappresentante per Stato membro, e porta quindi in dote elementi più tipici della dimensione intergovernativa. Forum consultivo e Gruppo di esperti indipendenti, invece, riuniscono esponenti di categorie di portatori di interessi e della società civile, oltre che soggetti qualificati: la composizione del primo, che vede coinvolte figure di diverso profilo, deve garantire un equilibrio tra interessi commerciali e non, mentre il secondo annovera personalità dalle comprovate competenze e conoscenze tecnico-scientifiche nel campo dell'IA.

Diverse sono anche le funzioni che gli organi in questione esercitano. È vero che tutti supportano l'attuazione e l'esecuzione del Regolamento fornendo assistenza e consulenza; tuttavia, il raggio di azione di Forum consultivo e Gruppo di esperti indipendenti è più circoscritto rispetto a quello del Consiglio per l'IA e, soprattutto, all'Ufficio per l'IA, presentato come il centro di competenze di tutta l'Unione nella materia di cui trattasi.

C'è però un collegamento evidente tra questi organi, dato dall'influenza della Commissione europea su di essi, non solo nella sua qualità di beneficiario principale delle rispettive attività. Il caso più eclatante è quello dell'Ufficio per l'IA, il quale, come si è anticipato poc'anzi, in pratica è parte della Commissione medesima. Tale organo di fatto non viene disciplinato dall'*AI Act*, che lo richiama soltanto, ma da una decisione della Commissione adottata addirittura prima del Regolamento[16], e già questa circostanza è molto singolare e sintomatica dei poteri che la Commissione può esercitare. Riguardo al Consiglio per l'IA, che in una certa misura serve anche da punto di raccordo per le autorità nazionali competenti, il grado di autonomia dalla Commissione è aumentato se si considera che il "comitato" elaborato nella proposta di Regolamento sull'IA avrebbe dovuto essere presieduto proprio da questa istituzione; l'*AI Act* riproduce tutt'altre logiche, giacché è uno dei rappresentanti degli Stati membri a presiedere l'organo, ma non sfugge che l'Ufficio per l'IA partecipa alle riunioni del Consiglio per l'IA e svolge al suo interno le funzioni di segretario. Più diretto è il rapporto tra Commissione, da una parte, e Forum consultivo e Gruppo di esperti indipendenti, dall'altra: è infatti la Commissione a nominare o selezionare i membri di entrambi gli organi e, nel caso del Gruppo di esperti, a determinarne l'istituzione con atto di esecuzione.

A fronte di questo nuovo impianto di *governance* sovranazionale, non va

[16] Dec. Comm. UE, 24 gennaio 2024, n. C/2024/1459, che istituisce l'Ufficio europeo per l'intelligenza artificiale, in G.U.U.E. C del 14 febbraio 2024, p. 1.

trascurato il ruolo giocato dal Garante europeo per la protezione dei dati (di seguito: Garante europeo o GEPD), designato quale autorità di vigilanza del mercato competente per le istituzioni, organi e organismi dell'Unione. Rispetto dunque alla definizione di "autorità di vigilanza del mercato" stabilita all'art. 3, par. 4, del Regolamento 2019/1020 applicabile negli Stati 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*.

Quanto ai suoi compiti, il Garante europeo è chiamato a monitorare l'applicazione dell'*AI Act* 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.

Il Regolamento attribuisce anche al GEPD il potere di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione in caso di violazione delle norme previste dall'*IA Act*. Questo "tesoretto" derivante dalle sanzioni 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, 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. Quest'ultimo, tuttavia, non prevede esplicitamente la possibilità per la Corte di giustizia di esaminare le sanzioni applicate dal Garante, sebbene possa venire in soccorso l'art. 64 del Regolamento 2018/1725 che riconosce alla Corte di giustizia il potere di estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.

Le constatazioni appena effettuate servono a tracciare la prima parte della traiettoria che spinge la disciplina del sistema di *governance* dell'*AI Act* ben al di fuori del predetto capo VII, riportandola a varie disposizioni che enunciano prerogative di prim'ordine della Commissione europea. Segnatamente, il Regolamento sull'IA si distingue per l'assegnazione alla Commissione di poteri in parte inconsueti a proposito dell'introduzione di obblighi *in itinere,* della possibilità di prendere decisioni specifiche e del controllo sui soggetti più prossimi ai rischi che la riforma mira a scongiurare o ridurre.

Il senso di questa evoluzione del ruolo della Commissione è da rinvenirsi nella selezione e nella gradazione, ad opera del legislatore dell'Unione, delle categorie di rischio e, per l'effetto, della scala di priorità

degli interventi da realizzare in sede di attuazione ed esecuzione. In altre parole, maggiore è il rischio sollevato dal sistema o dal modello di IA interessato, più intensi diventano i poteri che la Commissione può mettere in campo.

Stando al Regolamento, la Commissione può adottare atti delegati ed esecutivi, naturalmente in conformità agli artt. 290 e 291 TFUE. Può esercitare questi poteri normativi in una gamma piuttosto vasta di situazioni, andando tra l'altro a toccare punti sensibili (nevralgici?) dell'atto legislativo. Certo, l'art. 97 dell'*AI Act* afferma che la delega di potere ha una base di cinque anni e può essere revocata in qualsiasi momento da Parlamento europeo e Consiglio e l'art. 98 rinvia alla "procedura di comitato"[17]; sennonché, i limiti ai poteri normativi della Commissione sembrano alquanto tenui, soprattutto alla luce di una prassi ormai consolidata.

La *ratio* della delega di potere si rinviene specialmente nell'esigenza di efficientare la gestione dei rischi alti o sistemici, anche se la Commissione normalmente deve procedere previa valutazione di specifiche condizioni, talvolta assistite da criteri predefiniti. In particolare, la Commissione può adottare atti delegati modificare l'Allegato III dell'*AI Act*, incidendo sulle ipotesi previste o sui casi d'uso, come disposto dagli artt. 6, par. 6, e 7, par 1 e par. 3, del Regolamento. È sempre con atti delegati che la Commissione può decidere di rivedere la valutazione di conformità dei sistemi di IA ad alto rischio, aggiornando condizioni e procedure[18]. Analogamente, pure le regole applicabili ai modelli di IA per finalità generali con rischio sistemico *ex* art. 51 possono divenire oggetto di intervento della Commissione attraverso questa tipologia di misure; ciò eventualmente per cambiare criteri ed indicatori sostanziali per la designazione di tali modelli, nonché gli oneri che i rispettivi fornitori devono soddisfare con riguardo alla documentazione tecnica e alle informazioni da fornire[19].

L'approccio in discussione è completato da una serie di disposizioni che affidano alla Commissione il potere di adottare atti esecutivi. Un esempio è l'art. 41, par. 1, del Regolamento, che consente alla Commissione di stabilire, in determinate circostanze, specifiche comuni per i requisiti applicabili ai sistemi di IA ad alto rischio (artt. 8-15). In aggiunta, in forza dell'art. 56 la Commissione approva con atti di esecuzione i codici di buone pratiche, anche per conferirvi una validità generale all'interno dell'Unione[20]; laddove poi questi ultimi non siano stati resi disponibili in tempo utile, la Commissione può adottare atti di esecuzione per stabilire norme comuni circa l'attuazione degli obblighi a carico dei fornitori di modelli GPAI, compresi quelli ad alto rischio[21]. E ancora, anche il piano di monitoraggio successivo all'immissione sul mercato dei sistemi di IA ad alto rischio è stabilito tramite apposito atto di esecuzione della Commissione (art. 72, par. 3).

[17] Si tratta della procedura d'esame di cui all'art. 5 del Reg. (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, in G.U.U.E. L 55, 18 febbraio 2011, p. 13 (per quanto attiene all'adozione di atti di esecuzione).

[18] Art. 45, par. 5 e par. 6, *AI Act*. 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).

[19] Artt. 51, par. 3, 52, par. 4, 53, par. 5 e par. 6, oltre agli Allegati XI, XII e XIII *AI Act*.

[20] Art. 56, par. 6, *AI Act*.

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

Oltre a quanto appena indicato, la Commissione può esercitare altre prerogative importanti. Su tutte si segnalano le seguenti: decidere, se del caso *ex officio*, che un modello di IA per finalità generali debba essere classificato come modello a rischio sistemico, in base all'art. 51, par. 1, lett. b)[22]; stabilire, a norma dell'art. 46, par. 5 e par. 6, se sia giustificata o meno l'autorizzazione nazionale all'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; azionare la cosiddetta "procedura di salvaguardia dell'Unione", in virtù dell'art. 81, per intervenire in prima persona al fine di decidere sulla conformità di misure interne alle norme apicali del sistema di tutela contro i rischi cui l'*AI Act* è indirizzato.

Vanno infine richiamati i poteri di supervisione, indagine, esecuzione e monitoraggio in relazione ai fornitori di modelli GPAI, che competono esclusivamente alla Commissione. Gli artt. 88 ss. *AI Act* sanciscono prerogative di impatto potenzialmente notevole, dal momento che la Commissione può rivolgersi ai fornitori dei suddetti modelli anche per richiedere documenti e informazioni, compiere indagini, ordinare l'attuazione di misure.

A ciò si somma il potere di irrogare sanzioni pecuniarie, regolato dall'art. 101. La Commissione, infatti, può esercitare tale potere in numerose fattispecie, essendo sufficiente rilevare che una violazione intenzionale o negligente delle disposizioni del Regolamento applicabili ai fornitori dei modelli GPAI. Ed anche se la procedura prevede ovvie garanzie a favore dell'interessato, come il diritto di essere ascoltato, l'onere da parte della Commissione di rispettare il principio di proporzionalità e l'eventualità che la Corte di giustizia possa sindacare anche nel merito le decisioni con cui sono comminate le sanzioni, non va dimenticato che l'art. 101 stabilisce delle soglie massime alquanto elevate: fermo restando che ogni sanzione dovrà essere effettiva e dissuasiva, la Commissione potrà esigere pagamenti fino al 3% del fatturato mondiale annuo totale dell'esercizio precedente o a € 15 milioni, se superiore.

Da quanto precede si ricava l'attribuzione alla Commissione di una funzione di vigilanza a tratti "rafforzata", che trascende i poteri sanzionatori, diretti o mediati, espressamente previsi dai Trattati istitutivi: 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 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. E proprio a tale proposito, l'*AI Act* sviluppa ulteriormente l'approccio che innerva il DSA e il DMA, poiché, entro certi limiti, contempla meccanismi simili a quelli sviluppati dall'Unione nel corso del tempo nell'area del diritto *antitrust*.

IV. Attuazione dell'*AI Act* ed esigenze di leale cooperazione

Al di là dal ruolo predominante esercitato dalla Commissione europea, la struttura di *governance* illustrata richiede che i singoli attori coinvolti, e in particolare le autorità di vigilanza, interagiscano reciprocamente e garantiscano un elevato livello di cooperazione. Nello specifico, due sono gli scenari di interazione su cui vale la pena soffermarsi, anche a motivo dei collegamenti con il diritto UE in

[22] Si veda anche l'art. 52, par. 4, *AI Act*.

materia di concorrenza. Il primo scenario è riconducibile al rapporto tra autorità di vigilanza appartenenti al medesimo Stato membro e che potrebbero vantare una competenza in ordine all'applicazione dell'*AI Act*. 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.

IV.1 Monitoraggio interno e dimensione "orizzontale" della leale cooperazione

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[23]. 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 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[24]: 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 Regolamento 2016/679 e della direttiva (UE) 2016/680 (cd. direttiva polizia)[25].

Le riserve di competenza espressamente previste dal Regolamento sono finalizzate ad evitare che le attività di vigilanza sull'applicazione dell'*AI Act* 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[26]. 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 trat-

[23] Il Regolamento si riferisce, nello specifico, alla normativa relativa ai prodotti già sottoposti a controlli nel quadro del mercato interno.

[24] 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 36 ma non si ritrova nel testo del Regolamento.

[25] Dir. (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, G.U.U.E. L 119, 4 maggio 2016, p. 89.

[26] Reg. (UE) 2016/679, art. 22.

tamento di grandi quantitativi di dati sono alla base del funzionamento dell'intelligenza artificiale. Tuttavia, i diritti fondamentali che l'*AI Act* intende tutelare sono riconducibili ad un insieme più ampio, a seconda della tecnologia e dell'ambito di utilizzo. Per questo, a differenza di quanto auspicato dal Garante europeo nel parere emesso nel 2021[27], 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[28]. Nel caso di specie, si lamentava il fatto che l'interpretazione, da parte delle autorità antitrust, delle disposizioni del GDPR 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, 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[29]. 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 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.

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[30]. 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.

[27] 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.

[28] C. giust., 4 luglio 2023, C-252/21, *Meta platforms e a.*, ECLI:EU:C:2023:537, punto 44 ss.

[29] C. giust., *Meta platforms e a.*, punto 53.

[30] C. giust., 7 novembre 2013, C-518/11, *UPC Nederland BV v Gemeente Hilversum*, ECLI:EU:C:2013:709, punto 59; 1° agosto 2022, C-14/21 e C-15/21, *Sea Watch*, ECLI:EU:C:2022:604, punto 156.

IV.2 Monitoraggio multilivello e dimensione "verticale" della leale cooperazione

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 i competenti organi UE al fine di sorvegliare sulla corretta applicazione del Regolamento nei vari Stati membri e di elaborare linee guida in materia, specialmente in relazione ai modelli fondativi e modelli GPAI. 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 all'*AI Act* 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 Regolamento 2019/1020 e sotto il coordinamento dell'Ufficio per l'IA[31].

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 Regolamento 2019/1020. In aggiunta, l'*AI Act* 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.

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. Ciononostante, 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, specialmente 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.*[32]. 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*"[33], sottolineando l'importanza

[31] Peraltro, in riferimento alle presunte violazioni da parte di fornitori di modelli 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.

[32] C. giust., 15 giugno 2021, C-645/19, *Facebook Ireland e a.*, ECLI:EU:C:2021:483.

[33] Previsto dall'art. 60 del GDPR, tale meccanismo (denominato in italiano 'sportello unico') è stato poi incorporato e dettagliato nelle linee guida

di una cooperazione non solo efficace (come espressamente previsto dal GDPR) ma anche leale tra di loro. Ciò, per tornare al Regolamento sull'IA, 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[34]. 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.

Federico Ferri[*] – Susanna Villani[**]

Bibliografia

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 *Il ragionamento giuridico nell'era dell'intelligenza artificiale* (a cura di) S. Dorigo, Pisa, 2020, p. 1 ss.; A. Adinolfi, «Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione», in *I Post di AISDUE*, 15/2023, p. 321 ss.; S. Brettauer, «Extended powers for other supervisory authorities concerned in the case of cross-border data processing: Facebook Ireland», in *Common Market Law Review*, 2022, p. 1543 ss.; M. Carta, «Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte», in *Eurojus*, 2024, p. 188 ss.; F. Casolari, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020; G. Contaldi, «La proposta di Regolamento sull'intelligenza artificiale e la protezione dei dati personali», in *Verso una legislazione europea su mercati e servizi digitali*, (a cura di) G. Caggiano – G. Contaldi – P. Manzini, Bari, 2021, p. 207 ss.; G. De Gregorio – P. Dunn, «The European risk-based approaches: Connecting constitutional dots in the digital age», in *Common Market Law Review*, 2022, p. 473 ss.; P. De Pasquale, «Commento all'art. 4 TUE», in *Trattati dell'Unione europea*, Milano, 2014, (a cura di) A. Tizzano, p. 28 ss.; V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Pisa, 2023; A. Felice Uricchio – G. Riccio – U. Ruffolo (a cura di), *Intelligenza artificiale tra etica e diritti: prime riflessioni a seguito del libro bianco dell'Unione europea*, Bari, 2020; F. Ferri (a cura di), «Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive», in *Quaderni AISDUE* fascicolo speciale n. 2/2024; G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; L. Floridi, «The European Legislation on AI: a Brief Analysis of its Philosophical Approach», in *Philosophy & Technology*, 2021, p. 215 ss.; T. Frosini, «La privacy nell'era dell'intelligenza artificiale», in *DPCE Online*, 2022, p. 273 ss.; I. Graef, «Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment», in *Maastricht Journal of European and Comparative Law*, 2023, p. 325 ss.; C. Grieco, Intelligenza Artificiale e tutela degli utenti nel diritto

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.

[34] C. giust., *Facebook et al.*, sopra citata, punti 53, 60, 63, 72.

[*] Ricercatore in Diritto dell'Unione europea, *Alma Mater Studiorum* Università di Bologna (parr. I.1 – I.2 – III.2 – IV.2).

[**] 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 (parr. II.1 – II.2 – III.1 – IV.1).

dell'Unione europea, Napoli, 2023; G. Sartor – F. Lagioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliament Study, 2020; M. Klamert, «Article 4 TEU», in *The EU Treaties and the Charter of Fundamental Rights — A Commentary*, (eds.) M. Kellerbauer et al., Oxford, 2019, p. 35 ss.; P. Manzini, «Antitrust e privacy: la strana coppia», in *Quaderni AISDUE*, 2023, p. 196 ss.; A. Pajno – F. Donati – A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Vol. I, Diritti fondamentali, dati personali e regolazione*, Bologna, 2022; P.G. Picht, «CJEU on Facebook: GDPR Processing Justifications and Application Competence», in *Gewerblicher Rechtsschutz und Urheberrecht*, 2023, p. 1169 ss.; O. Pollicino, «Potere digitale», in *Enciclopedia del diritto – I tematici - Potere e Costituzione*, (a cura di) M. Cartabia – M. Ruotolo, Milano, 2023, p. 410 ss.; G. Resta, «Cosa c'è di "europeo" nella proposta di Regolamento UE sull'Intelligenza Artificiale?», in *Diritto dell'informazione e dell'informatica*, 2022, p. 323 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. 435 ss.; U. Ruffolo (a cura di), *XXVI lezioni di Diritto dell'Intelligenza Artificiale. Saggi a margine del ciclo seminariale "Intelligenza Artificiale e diritto"*, Torino, 2020; C. Schepisi, «Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di Regolamento della Commissione», in *I Post di AISDUE*, 2023, p. 330 ss.; A. Simoncini, «La proposta di regolamentazione dell'intelligenza artificiale. Prime riflessioni», in Protezione dei dati personali, e nuove tecnologie, in *Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche* (a cura di) A. Adinolfi – A. Simoncini, Napoli, 2022, p. 1 ss.; A. Simoncini – G. Sartor – G. De Gregorio – O. Pollicino – A. Reichman – H. Micklitz (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge 2022.