RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0155 • articolo sottoposto a peer review • pubblicato in anteprima il 6 giu. 2024

PIETRO FALLETTA – ANNALISA MARSANO

Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR

La pervasività dei sistemi di intelligenza artificiale e il relativo impatto in termini di protezione dei dati personali impongono una profonda riflessione sulle recenti scelte normative del legislatore europeo e, in prospettiva, di quello nazionale. In questo senso, il contributo delinea, in primo luogo, l'attuale quadro legislativo europeo in materia di dati e IA, sullo scenario della complessa dimensione geopolitica in materia. Muovendo da queste premesse, il lavoro traccia un'analisi in chiave sistemica del Regolamento europeo sull'intelligenza artificiale (c.d. "AI Act"), evidenziando luci ed ombre del complesso rapporto con il Reg. (UE) n. 2016/679 ("GDPR") e identificando analogie e differenze tra i due atti normativi. Il contributo analizza, quindi, in ottica comparata, il sistema sanzionatorio e l'apparato di governance definiti dall'AI Act, focalizzandosi sulla delicata scelta di un'autorità di controllo nazionale per regolare l'intelligenza artificiale in Italia. Infine, gli autori formulano alcune riflessioni conclusive sui principali nodi tematici emersi nel corso della trattazione e propongono una prospettiva *de iure condendo* alla luce dell'analisi svolta.

AI Act – Intelligenza artificiale – Unione europea – Privacy – GDPR – Protezione dei dati personali

Artificial intelligence and data protection: the interplay between the European Artificial Intelligence Regulation and the GDPR

The widespread use of artificial intelligence systems and its impact on personal data protection calls for a thorough investigation of the regulatory governance adopted in this field by the European lawmaker and, in perspective, by the national one. In this sense, this paper first outlines the current European legislative framework on data and artificial intelligence, also tackling the related geopolitical dimension of the issue. The work then draws a systemic analysis of the recently approved European Regulation on Artificial Intelligence (so-called "AI Act"), showing lights and shadows of the complex interplay with (EU) Reg. no. 2016/679 ("GDPR") and identifying similarities and differences between the two regulatory acts. The paper goes on to examine, from a comparative perspective, the sanctioning system and the governance framework defined by the AI Act, focusing on the difficult choice of a national supervisory authority to regulate artificial intelligence in Italy. Finally, the authors provide some closing remarks on the most significant challenges raised in the context of the paper and propose some *de iure condendo* perspectives in the light of the studies carried out on the matter.

AI Act – Artificial Intelligence – European Union – Privacy – GDPR – Data protection

Pietro Falletta è ricercatore di Diritto amministrativo presso l'Università dell'Insubria; Annalisa Marsano è funzionario giuridico presso l'Autorità garante per la protezione dei dati personali (la partecipazione a questa attività è a titolo personale). Il presente contributo è frutto della piena condivisione di idee ed opinioni tra gli Autori. La stesura dei paragrafi 1 e 2 si deve ad Annalisa Marsano, quella dei paragrafi 3 e 4 a Pietro Falletta. Il paragrafo 5 è l'esito di una stesura condivisa.

Sommario: 1. Dalla strategia europea sui dati al Regolamento europeo sull'intelligenza artificiale. – 2. Il delicato rapporto tra il Regolamento europeo sull'intelligenza artificiale e il GDPR. – 3. Il sistema sanzionatorio dell'AI Act: luci ed ombre. – 4. Il sistema di governance dell'AI Act: la delicata scelta di un'autorità di controllo nazionale per regolare l'intelligenza artificiale. – 5. Conclusioni.

1. Dalla strategia europea sui dati al Regolamento europeo sull'intelligenza artificiale

L'uso sempre più frequente di strumenti tecnologici supportati da sistemi di intelligenza artificiale ha profondamente innovato le relazioni umane, così come le metodologie di apprendimento e le modalità di azione del decisore pubblico[1]. In tal senso, il ricorso a strumenti di IA rappresenta una delle maggiori sfide per l'evoluzione degli strumenti di regolazione, sia per l'estrema varietà di soluzioni possibili, sia in ragione dei numerosi rischi che l'applicazione di queste tecnologie comporta[2].

Il fenomeno si colloca nell'ambito di un preciso quadro normativo europeo, che prende le mosse dalla c.d. Strategia europea sui dati 2030, varata dalla Commissione europea nel 2020[3] con l'intento di realizzare un unico sistema normativo applicabile in tutta Europa, atto a disciplinare l'economia dei dati, nonché a prevenire rischi e abusi derivanti dalla posizione dominante delle grandi piattaforme online. Le scelte del legislatore europeo al centro della Strategia riguardano, *inter alia*, la disponibilità, l'interoperabilità e la condivisione dei dati, una maggior chiarezza sulle facoltà di utilizzo dei dati stessi, la governance dei processi, la creazione di spazi comuni europei.

La Strategia europea dev'essere, quindi, interpretata come lo strumento attraverso cui l'Unione europea si è impegnata nell'avviare una concreta azione legislativa avente ad oggetto l'istituzione di un mercato unico europeo dei dati conforme ai principi su cui si fonda l'Ue.

Ciò rende evidente come l'ordinamento giuridico europeo, dopo aver formalmente riconosciuto il diritto alla protezione dei dati personali attraverso l'art. 8 della Carta dei diritti fondamentali dell'Ue, giunga ora ad incoraggiare il mercato dei dati (personali e non), con il precipuo scopo di impedire che le imprese dell'Unione possano perdere competitività dinanzi alle logiche proprietarie tipiche dei mercati extra-europei[4]. Le riflessioni in merito alla Strategia europea sul digitale e sull'intelligenza artificiale devono muovere, dunque, dalla concezione dei dati quale nuova valuta[5] e oggetto di scambio nel mercato digitale, elemento necessario per comprendere la *ratio* seguita dal legislatore europeo nel disciplinare la materia[6]. In questo senso, nella perenne esigenza di equilibrio tra il perseguimento della competitività del mercato europeo e la tutela dei principi fondamentali della persona, emerge la rilevanza, anche patrimoniale, dei dati.

1. In tal senso, cfr. van den Hoven van Genderen 2017.
2. Ciaralli 2023, pp. 41-42.
3. Commissione europea, *Una strategia europea per i dati*, COM (2020)66, 19 febbraio 2020.
4. Bravo 2021, pp. 200-202.
5. Eggers-Hamill-Ali 2013.
6. Peluso 2023.

Questo obiettivo – ancora oggi al centro dell'impegno delle istituzioni europee – viene perseguito attraverso un pacchetto di norme che regolano il fenomeno del mercato unico dei dati sotto diversi aspetti, tra di loro interconnessi:

- *Data Governance Act*[7]: volto ad individuare processi e strutture per favorire la disponibilità dei dati (personali e non) tramite il riutilizzo dei dati della PA e la condivisione dei dati tra imprese attraverso gli *European Data Spaces*;
- *Data Act*[8]: volto ad integrare il *Data Governance Act*, chiarendo chi e a quali condizioni possa creare valore dai dati;
- *Digital Services Act*[9]: volto a proteggere lo spazio digitale dalla diffusione di beni, contenuti e servizi illegali e garantire la protezione dei diritti fondamentali degli utenti;
- *Digital Markets Act*[10]: volto a contrastare gli abusi di mercato delle grandi piattaforme digitali in Europa e finalizzato a limitare gli squilibri economici e le pratiche commerciali sleali dei *Gatekeeper* (gestori di servizi digitali);
- *Artificial Intelligence Act*: volto a promuovere la diffusione di un'IA affidabile e garantire un livello elevato di protezione dei diritti fondamentali dell'individuo, sostenendo nel contempo l'innovazione e il miglioramento del mercato interno[11].

Ognuno degli atti sopra riportati presenta la forma di regolamento e, pertanto, è anzitutto indirizzato ad una piena armonizzazione delle relative discipline[12].

In tale contesto, il legislatore europeo è intervenuto, per primo a livello mondiale, a disciplinare l'intelligenza artificiale, dando vita al Regolamento proposto dalla Commissione europea nell'aprile 2021 e finalizzato a stabilire regole armonizzate in materia di IA (di seguito, il "Regolamento" o "AI Act")[13].

Il Regolamento persegue il duplice obiettivo del Libro bianco sull'intelligenza artificiale[14] di promuovere l'adozione dell'IA ed affrontare i rischi associati all'utilizzo di tale tecnologia, allo scopo di sviluppare un ecosistema di fiducia attraverso un quadro giuridico per un'IA affidabile[15].

In via generale, il Regolamento prevede che la disciplina europea dell'IA sia equilibrata e proporzionata, evitando di limitare eccessivamente lo sviluppo delle nuove tecnologie ed evidenziando allo stesso tempo i rischi che possono derivare da determinati utilizzi dei sistemi di intelligenza artificiale[16]. Il quadro normativo relativo all'intelligenza artificiale dovrà essere, pertanto, in grado di assicurare che tali sistemi siano utilizzati nel rispetto dei valori dell'Unione europea e del diritto attualmente vigente, nonché garantire che

7. 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).
8. Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).
9. 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 (regolamento sui servizi digitali).
10. 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 (regolamento sui mercati digitali).
11. Finocchiaro-Pollicino 2022.
12. Cerrina Feroni 2022.
13. Cfr. 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) 206 come successivamente modificata nel corso della procedura 2021/0106 (COD) conclusa con l'approvazione del Parlamento europeo.
14. Sul punto, cfr. Pacileo 2022, pp. 305 e 306.
15. Commissione europea, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65), 19 febbraio 2020.
16. Al riguardo, si veda, tra gli altri, Scherer 2016, p. 365.

i cittadini europei possano beneficiare delle nuove tecnologie di IA senza rinunciare ai valori e i principi che caratterizzano il sistema giuridico comune.

Una riflessione organica sulla regolamentazione della complessa materia dell'intelligenza artificiale richiede anzitutto una definizione, non certo agevole, dell'oggetto in questione[17], specie in un'ottica di correlazione con il fenomeno giuridico[18]. Al riguardo, occorre, anzitutto, domandarsi se fosse opportuno per il legislatore adottare un approccio diretto a disciplinare l'intelligenza artificiale nel suo complesso o, piuttosto, regolare le applicazioni dell'intelligenza artificiale in singoli settori o materie. La prima opzione è proprio quella percorsa dall'AI Act che ha, infatti, un approccio normativo orizzontale e si basa su una nozione molto estesa di intelligenza artificiale. Nello specifico, l'art. 3 del Regolamento definisce un sistema di IA come «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»[19].

Il Regolamento include, dunque, nel concetto di intelligenza artificiale quei sistemi che, per obiettivi espliciti o impliciti, deducono, dagli input ricevuti, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali, restando invece esclusi i software di natura meno complessa, nonché i sistemi di IA utilizzati esclusivamente per scopi militari, di difesa, di ricerca e innovazione, ovvero per usi non professionali[20].

Tale definizione – in linea con quella proposta in ambito OCSE[21] – appare volutamente generica ed ampia, in modo da risultare quanto più possibile neutrale e così mitigare il pericolo di una rapida obsolescenza della normativa.

La scelta del regolatore europeo di adottare un approccio normativo orizzontale ha anche uno specifico peso geopolitico nello scacchiere internazionale. A ben vedere, come si evince dalla lettura della relazione introduttiva al Regolamento, l'interesse primario dell'Ue è quello di «tutelare la sovranità digitale dell'Unione e sfruttare gli strumenti e i poteri di regolamentazione di quest'ultima per plasmare regole e norme di portata globale». Nel panorama geopolitico attuale, quindi, la strategia dell'Unione consiste, non soltanto, nell'imporsi come leader nella produzione normativa[22], ma anche nel rendere il modello europeo un riferimento globale atto ad essere implementato in tutto il resto del mondo[23], come già accaduto in passato con la normativa sulla protezione dei dati contenuta nel Regolamento (UE) n. 2016/679 ("GDPR") (si parla in questo caso di "effetto Bruxelles")[24].

In ottica comparata, è utile infatti rammentare che il Regolamento in esame si pone essenzialmente all'interno di un contesto internazionale caratterizzato dall'assenza di una disciplina organica in materia[25]. Per questa via, v'è da considerare che i principali *competitor* su scala mondiale nel settore dell'intelligenza artificiale, ossia Cina e Stati Uniti, seppure già dotati di una regolazione in materia in grado di fungere da mezzo attraverso cui

17. Sul punto, cfr. Floridi-Cowls 2019.
18. Finocchiaro 2022, pp. 1085-1087.
19. Art. 3, n. 1 Regolamento Ue sull'intelligenza artificiale.
20. Per un'analisi definitoria del concetto di intelligenza artificiale si veda, *inter alia*, Pagallo 2017.
21. «Machinebased system that can, for a given set of humandefined objectives, make predictions, recommendations or decisions influencing real or virtual environments. It uses machine and/or humanbased inputs to perceive real and/or virtual environments; abstract such perceptions into models (in an automated manner e.g. with ML or manually); and use model inference to formulate options for information or action. AI systems are designed to operate with varying levels of autonomy», in OECD 2019.
22. In tal senso Veale-Matus-Gorwa 2023, p. 263.
23. Resta 2022, pp. 328 e 329.
24. Si veda al riguardo Bradford 2021.
25. Casonato-Fasan-Penasa 2022, p. 178.

promuovere e favorire lo sviluppo dell'IA, presentano, tuttavia, normative frammentate e per certi versi lacunose[26]. Da un lato, negli USA[27], la strategia prescelta sembrerebbe prediligere un approccio normativo soft, dettato dal timore che un eccessivo rigore regolatorio possa impedire il pieno sviluppo dell'IA[28]; dall'altro, la Cina ha inaugurato un quadro legislativo autoritario volto a promuovere un elevato sviluppo economico dell'IA ma contraddistinto da numerose lacune in termini di protezione dei dati personali[29] e da una quasi totale mancanza di trasparenza informativa[30].

D'altro canto, il limite tecnico-giuridico da riconoscere rispetto all'approccio regolatorio scelto dal legislatore europeo è rinvenibile nel fatto che le norme del Regolamento non risolvono specifici problemi né colmano precise lacune dell'ordinamento, ma trovano applicazione rispetto a qualsiasi settore della società civile, dall'ambito sanitario a quello finanziario.

Quanto all'ambito di applicazione soggettiva dell'AI Act, rileva in primo luogo la natura extra-territoriale della nuova regolamentazione. Infatti, il Regolamento si applicherà anche nei confronti dei soggetti e delle organizzazioni extra-europee, sia nel caso in cui questi abbiano uno stabilimento all'interno dell'Unione europea, sia nell'ipotesi in cui essi – pur in assenza di uno stabilimento – offrano beni o servizi nel mercato unico[31]. Più nel dettaglio, i destinatari di questo Regolamento sono prevalentemente fornitori ("*provider*") ed utilizzatori ("*deployer*") di sistemi di IA, seguiti poi da: importatori e distributori; produttori di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; rappresentanti autorizzati di fornitori che non sono stabiliti in Ue; persone interessate che si trovano nell'Unione europea.

In relazione ai principali destinatari dell'AI Act, è bene tenere presente che i fornitori – persone fisiche o giuridiche – sono coloro che sviluppano o fanno sviluppare un sistema di IA e che lo immettono poi sul mercato o in servizio[32], mentre gli utilizzatori sono coloro che utilizzano i sistemi di intelligenza artificiale. L'interazione tra fornitori ed utilizzatori costituisce il nodo centrale della ripartizione delle responsabilità nell'ambito del Regolamento. Si noti che, nell'ambito di questa relazione, l'utilizzatore non è soltanto la persona fisica che si rapporta con l'IA per ricevere un servizio, ma «persona fisica o giuridica, autorità pubblica, agenzia o 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»[33]. Conseguentemente, le società che non hanno come business quello di sviluppare o vendere tecnologia basata sull'intelligenza artificiale vanno considerate alla stregua di utilizzatori.

In relazione all'approccio adottato, il Regolamento ricorre al c.d. *risk-based approach* per classificare e categorizzare i principali sistemi di IA[34] in uso secondo una struttura piramidale fondata su quattro distinti livelli di rischio determinati dall'uso di un dato sistema: (i) rischio inaccettabile; (ii) rischio alto; (iii) rischio basso o minimo; (iv) rischio specifico per la trasparenza. L'approccio *risk-based* introduce restrizioni ed obblighi a cui attenersi a seconda del grado di rischio che una determinata applicazione può presentare per i singoli e per la società[35].

26. Alù 2023.
27. Marchetti-Parona 2022.
28. Sul punto, si veda il piano *Innovate in America*. Con diverse prospettive, fra gli altri, Burt 2021; Aaronson 2020.
29. Sul punto, si veda *New Generation Artificial Intelligence Development Plan* (AIDP), su cui, fra gli altri, Roberts et al. 2021.
30. A tal proposito, Chiti-Marchetti 2020; Cath et al. 2018.
31. Art. 2, par. 1, Regolamento Ue sull'intelligenza artificiale
32. Art. 3, n. 3, Regolamento Ue sull'intelligenza artificiale.
33. Art. 3, n. 4, Regolamento Ue sull'intelligenza artificiale.
34. Mantelero 2022, p. 141.
35. AA.VV. 2023.

Secondo il modello di gestione del rischio sopra rappresentato, il Regolamento distingue i sistemi come segue:

Sistemi di IA con rischio inaccettabile: il Regolamento vieta espressamente tutte quelle pratiche il cui livello di rischio sia da ritenersi inaccettabile, in quanto contrarie ai principi ispiratori dell'ordinamento dell'Ue. Tra i trattamenti vietati dal Regolamento si annoverano[36]:

- punteggio sociale, per finalità pubbliche e private;
- sfruttamento delle vulnerabilità delle persone, utilizzo di tecniche subliminali;
- identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità di contrasto, fatte salve limitate eccezioni;
- categorizzazione biometrica delle persone fisiche sulla base di dati biometrici per dedurne o desumerne la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale; sarà ancora possibile filtrare set di dati basandosi su dati biometrici nel settore delle attività di contrasto;
- polizia predittiva su singoli;
- riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, eccetto per motivi medici o di sicurezza (ad esempio, il monitoraggio dei livelli di stanchezza di un pilota);
- estrazione non mirata di immagini facciali da Internet o telecamere a circuito chiuso per la creazione o l'espansione di banche dati[37].

Sistemi di IA ad alto rischio: sono quelli che implicano o possono implicare un alto rischio per la salute e la sicurezza o per i diritti fondamentali delle persone fisiche, trovando così applicazione il Titolo III del Regolamento. Questi sistemi non sono di per sé vietati, ma il loro utilizzo è subordinato al rispetto di determinati requisiti obbligatori, nonché ad una duplice valutazione *ex ante*, ossia una valutazione di impatto sui diritti fondamentali ed una di conformità rispetto alla normativa applicabile[38].

La valutazione d'impatto sui diritti fondamentali (c.d. *Fundamental Rights Impact Assessment* – FRIA) – obbligo che il Regolamento pone in capo ai *deployer* – ha la finalità di valutare le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema, la conformità del sistema con il diritto europeo e nazionale in materia di diritti fondamentali e l'impatto ragionevolmente prevedibile sui medesimi[39]. La valutazione di conformità (c.d. *conformity assessment*), invece – obbligo attribuito dal Regolamento ai provider – presuppone un'analisi di conformità del sistema di IA rispetto ai requisiti richiesti dall'AI Act. La procedura di valutazione dovrà essere costituita dalle seguenti fasi: (i) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema; (ii) stima e valutazione dei rischi che possono emergere quando il sistema è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; (iii) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato; (iv) adozione di adeguate misure di gestione dei rischi che tengono in debita considerazione gli effetti e le possibili interazioni derivanti dall'applicazione combinata degli elementi indicati sopra alla luce dello stato dell'arte generalmente riconosciuto[40].

Ad ogni buon conto, si fa notare che siffatte operazioni di valutazione si traducono per le aziende in ingenti costi e risorse. Infatti, il bilanciamento dei diritti, così come l'analisi della compliance di un sistema di IA, rappresenta un'operazione complessa finanche per giuristi, con la conseguenza che fornitori ed utilizzatori sarebbero costretti ad esternalizzare lo svolgimento di tali valutazioni, avvalendosi di soggetti terzi qualificati. In ogni caso, anche qualora *provider* e *deployer* fossero in grado di sostenere i costi che ne deriverebbero, questi sarebbero comunque responsabili di decisioni sensibili. Non è, dunque, possibile eseguire

36. Art. 5, par. 1, Regolamento Ue sull'intelligenza artificiale.
37. Commissione europea 2023.
38. Art. 6, par. 1, Regolamento Ue sull'intelligenza artificiale.
39. Art. 27, Regolamento Ue sull'intelligenza artificiale.
40. Artt. 16 e 43 Regolamento Ue sull'intelligenza artificiale.

queste valutazioni in assenza di linee guida di settore che forniscano le corrette istruzioni da seguire. La mancanza di adeguate linee guida – necessarie a fare da bussola in analisi articolate come quelle in commento – porterebbe all'insorgere di prassi auto-regolamentative ed eccessivamente discrezionali dei destinatari di tali obblighi[41]. Inoltre, il Regolamento stabilisce che i sistemi di IA ad alto rischio devono essere progettati e sviluppati in modo tale da assicurare la tracciabilità del relativo funzionamento, che dovrà essere sufficientemente trasparente da permettere agli utilizzatori di interpretarne l'output e utilizzarlo adeguatamente[42]. I medesimi sistemi dovranno, peraltro, essere progettati in modo tale da garantire un adeguato livello di accuratezza, robustezza e cybersicurezza[43]. Gli stessi – secondo il Regolamento – dovranno essere sviluppati con strumenti di interfaccia uomo-macchina in grado di assicurare una valida supervisione da parte delle persone fisiche diretta a prevenire e contrastare i rischi per la salute, la sicurezza o i diritti fondamentali[44]. Di solito, i sistemi di IA ad alto rischio vengono utilizzati nell'ambito di dispositivi medici, veicoli, processi di recruiting, infrastrutture critiche, accesso a servizi pubblici o privati essenziali.

Sistemi di IA a rischio basso o minimo: vengono individuati per differenza rispetto ai sistemi a rischio inaccettabile o alto. Nello specifico, i sistemi di IA che comportano un rischio basso o minimo sono tutti quei sistemi leciti, chiamati esclusivamente a rispettare alcuni minimi requisiti di trasparenza. In particolare, il Regolamento richiede che il fornitore si preoccupi che la persona esposta ad un sistema di IA sia informata, in modo puntuale, chiaro e comprensibile, di stare interagendo con un sistema di IA. Inoltre, "qualora necessario", devono essere indicate quali funzioni il sistema esercita, se esiste un controllo sul sistema stesso da parte di una persona fisica, l'identificativo del responsabile del sistema, l'indicazione dei diritti della persona esposta e le azioni che la persona esposta può adottare per opporsi all'uso del sistema di IA[45]. In aggiunta ai doveri dei fornitori, il Regolamento prescrive specifici obblighi anche in capo agli utilizzatori di sistemi di IA ad alto rischio[46]. Gli utilizzatori sono, infatti, tenuti ad assicurare la correttezza e la qualità dei dati utilizzati dal sistema. Inoltre, gli utilizzatori devono rispettare le istruzioni del fornitore ma, laddove ritengano che l'uso in conformità alle istruzioni presenti un rischio, dovranno comunicarlo al fornitore stesso e, nel caso in cui quest'ultimo sia irreperibile, l'utilizzatore dovrà notificare l'incidente o il malfunzionamento alla competente autorità di controllo.

Sistemi di AI con specifici rischi di trasparenza: sistemi in relazione ai quali gli operatori devono adempiere ad obblighi sostanzialmente meno onerosi, prevalentemente di natura informativa (ad esempio, in relazione all'uso di chatbot, chiarendo agli utenti che stanno conversando con una macchina).

Con specifico riferimento ai sistemi di IA ad alto rischio, il Regolamento stabilisce, inoltre, che i fornitori debbano garantire la conformità dei propri sistemi di intelligenza artificiale ai requisiti fissati dalla normativa in esame[47]. Inoltre, una volta classificati i propri sistemi di IA come ad alto rischio, i *provider* saranno chiamati a registrare tali sistemi nella banca dati istituita a livello europeo e gestita dalla Commissione europea, di cui si dirà meglio nel prosieguo[48].

Nell'ipotesi in cui il fornitore ritenga che il proprio sistema non determini un rischio significativo tale da classificare il sistema stesso come ad alto rischio, dovrà documentare dettagliatamente la propria valutazione prima di immettere sul mercato il relativo sistema e rendere disponibile tale documentazione su richiesta dell'autorità

41. Novelli 2024, p. 100 ss.
42. Art. 13, Regolamento Ue sull'intelligenza artificiale.
43. Art. 15, Regolamento Ue sull'intelligenza artificiale.
44. Art. 14, par. 1, Regolamento Ue sull'intelligenza artificiale.
45. Considerando 72 nonché art. 13 Regolamento Ue sull'intelligenza artificiale.
46. Art. 26, Regolamento Ue sull'intelligenza artificiale.
47. Art. 8, Regolamento Ue sull'intelligenza artificiale.
48. Art. 49, Regolamento Ue sull'intelligenza artificiale.

di controllo competente a livello nazionale[49]. A seguito dell'immissione in commercio dei propri prodotti, i fornitori dei sistemi di IA ad alto rischio saranno chiamati a predisporre un programma di monitoraggio post-vendita proporzionato ai rischi del sistema immesso[50]. In tal senso, sarà allora necessaria un'analisi dei dati sulle prestazioni del sistema per l'intera durata di utilizzo del prodotto, in modo da verificarne la continua conformità con il Regolamento. Nei successivi dieci anni dall'immissione del prodotto, i provider dovranno anche conservare la documentazione tecnica, quella relativa al sistema di *quality management* e quella riguardante eventuali cambiamenti approvati dalle autorità competenti[51]. Infine, qualora un fornitore di sistemi di IA ad alto rischio ritenga che il proprio sistema, già immesso sul mercato, non sia più in linea con i requisiti previsti dal Regolamento, dovrà senza ingiustificato ritardo ritirarlo dal mercato o renderlo conforme alla normativa, nonché informare i relativi distributori e le autorità competenti. Allo stesso modo, quando un fornitore venga a conoscenza dell'esistenza di un rischio nel proprio sistema, sarà tenuto ad informare immediatamente l'autorità nazionale competente, specificando la causa della non ottemperanza e le relative azioni correttive avviate[52].

D'altro canto, anche gli utilizzatori dei sistemi ad alto rischio sono depositari di specifici obblighi da osservare. Essi sono, infatti, tenuti ad osservare le istruzioni per l'uso predisposte dal fornitore del sistema di IA, oltre che ad assicurare la correttezza dei dati di input tramite cui alimentare il sistema di intelligenza artificiale, monitorare il funzionamento del sistema di IA e segnalare eventuali rischi ed incidenti al fornitore stesso. Inoltre, gli utilizzatori sono chiamati a conservare i log dei sistemi di cui si avvalgono. Il Regolamento statuisce che – ove non diversamente previsto – tali log debbano essere conservati per un periodo di tempo non inferiore a sei mesi, precisando che, in ogni caso, dovranno essere tenuti per un tempo adeguato rispetto alla finalità del sistema e degli obblighi giuridici applicabili. Infine, gli utilizzatori di sistemi di IA ad alto rischio dovranno eseguire una valutazione d'impatto sul trattamento dei dati personali (c.d. DPIA ovvero *Data Protection Impact Assessment*) ai sensi dell'art. 35 del GDPR, avvalendosi delle informazioni che i fornitori hanno l'obbligo giuridico di rendere disponibili agli utilizzatori stessi[53].

2. Il delicato rapporto tra il Regolamento europeo sull'intelligenza artificiale e il GDPR

Il Regolamento sull'IA non è, come accennato, un atto legislativo *stand-alone*, ma si inserisce nell'ambito di una cornice normativa europea complessa e frastagliata, dove, al fine di garantire la certezza del diritto, è chiamato a coordinarsi con altre discipline proposte dalla Commissione in materia di dati e trasformazione digitale[54]. Sotto questo profilo, il grado di complessità aumenta se si considera che l'applicazione del Regolamento dovrà trovare un adeguato coordinamento anche rispetto al GDPR, data la stretta interrelazione *ratione materiae*. È chiaro, infatti, che i sistemi di intelligenza artificiale, per raggiungere un elevato grado di rendimento, necessitano di una grande mole di dati, e più è ampia la quantità di dati posta a disposizione di questi sistemi, tanto più precise sono le previsioni elaborate dagli stessi[55]. Conseguentemente, la fase più delicata per il corretto funzionamento di un sistema di intelligenza artificiale è proprio quella di raccolta dei dati[56].

Al riguardo, il Regolamento sull'intelligenza artificiale non si occupa della raccolta e del trattamento dei dati, i quali rimangono pertanto regolati dalla normativa vigente e, in particolare, dal GDPR. Trascorso, dunque, il momento di raccolta dei dati, è fondamentale comprendere quale sia la

49. Art. 16, Regolamento Ue sull'intelligenza artificiale.
50. Art. 72, Regolamento Ue sull'intelligenza artificiale.
51. Artt. 16 e 18, Regolamento Ue sull'intelligenza artificiale.
52. Art. 20, Regolamento Ue sull'intelligenza artificiale.
53. Art. 26, Regolamento Ue sull'intelligenza artificiale.
54. Iacovelli-Fontana 2022, pp. 117-119.
55. Finocchiaro 2019.
56. Si veda, al riguardo, Colapietro-Moretti 2020, pp. 376-377.

normativa applicabile, una volta che tali dati vengano immessi nel sistema.

Considerati gli ampi margini di potenziale sovrapposizione, l'attuazione delle due discipline potrebbe portare ad un eccesso di regolamentazione. Per questo motivo, il rapporto simbiotico tra protezione dei dati personali e intelligenza artificiale deve porsi al centro dell'esame e della relativa attuazione dell'AI Act, al fine di prevenire eventuali contrasti o contrapposizioni con la disciplina complementare del GDPR[57]. Con specifico riguardo a questo punto, la stessa Commissione europea, nella propria relazione esplicativa di accompagnamento del Regolamento sull'IA, chiarisce che quest'ultimo non pregiudica l'applicabilità del GDPR. È una considerazione in qualche modo ovvia, dal momento che il GDPR è finalizzato a proteggere un diritto fondamentale, già previsto dagli articoli 8 della Carta dei diritti fondamentali dell'Unione europea e 16 TFUE[58]. Da una tale constatazione deriva che non sarebbe possibile risolvere eventuali conflitti tra fonti normative invocando il principio di specialità. Invero, non avrebbe senso sostenere la prevalenza del Regolamento sull'intelligenza artificiale rispetto al GDPR sulla base di un principio di specialità, considerato che la seconda normativa è volta ad attuare un diritto umano fondamentale espressamente previsto da una fonte primaria. Si può, dunque, affermare che entrambe le fonti in esame dovranno essere applicate ed implementate cumulativamente tra loro[59].

Inevitabilmente, dunque, il Regolamento sull'IA e il GDPR presentano numerosi punti di contatto rispetto alle proprie modalità di regolazione. Le similitudini tra le due fonti normative si riscontrano già nello strumento giuridico prescelto dal legislatore europeo: in entrambi i casi, l'Unione europea ha adottato la forma del regolamento in luogo della direttiva, al fine di consolidare un quadro normativo omogeneo e prevalentemente rigido per gli Stati Membri, prevedendo sempre meccanismi di revisione periodica per assicurare discipline "*stable but not still*"[60]. La scelta della fonte utilizzata, come è evidente, costituisce un fil rouge che collega tutti gli atti normativi della politica europea sul digitale, in linea con la volontà di inaugurare una governance dell'innovazione incentrata sul principio del "*one continent, one law*"[61].

Altra analogia tra i due testi normativi è, certamente, la scelta della medesima cornice strutturale che fa da sfondo alle relative discipline, ossia il c.d. *risk based approach* (fondato su di una piramide di gravità ascendente), dove sono le stesse organizzazioni a dover dimostrare la propria conformità al dettato legislativo. In tal senso, come già evidenziato, l'AI Act classifica i sistemi di intelligenza artificiale in base al rischio generato per gli utilizzatori, fissando specifici obblighi per fornitori ed utilizzatori di entità crescente in base al livello di rischio considerato. In particolare, in analogia con gli artt. 25 e 35 del GDPR, l'AI Act impone ai *provider* di implementare un sistema di gestione del rischio atto a mappare i rischi conosciuti e quelli prevedibili e a mitigarli, di informare gli interessati della loro esistenza, nonché di monitorare ed aggiornare in via periodica il sistema di *risk assessment*. La valorizzazione dell'autonoma valutazione dell'operatore risponde ad una logica di responsabilizzazione e *accountability* già centrale nell'impianto giuridico del GDPR[62].

Ciononostante, i punti di contatto con il GDPR non si esauriscono nell'approccio basato sul rischio: infatti, il Regolamento richiama anche principi e meccanismi tipici del sistema di governance e di gestione dei dati del GDPR, impiegandoli come strumenti per un corretto e trasparente addestramento dei sistemi di IA[63]. Tra questi, si riportano di seguito i principali elementi in comune.

Extraterritorialità: l'AI Act persegue anche obiettivi di natura geopolitica, cercando di estendere l'ambito di applicazione del Regolamento. L'art. 2, infatti, con tecnica analoga a quella utilizzata

57. Cerrina Feroni 2023.
58. Si veda, a tal proposito, Pollicino-Bassini 2017, pp. 135-136; Calzolaio 2017, p. 594.
59. Contaldi 2021, p. 1199 ss.
60. Casonato-Marchetti 2021, pp. 419-421.
61. Commissione Europea 2015.
62. Mantelero-Poletti 2018, p. 73.
63. AssoDPO 2023.

dall'art. 3 del GDPR, dispone che il Regolamento si applichi ai fornitori che immettono sul mercato o mettono in servizio sistemi di intelligenza artificiale nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un Paese terzo, nonché agli utilizzatori dei sistemi di IA situati nell'Unione e ai fornitori e agli utilizzatori di sistemi di IA situati in un Paese terzo, ove l'output prodotto dal sistema sia utilizzato nell'Unione.

Qualità ed esattezza dei dati: quello della qualità e dell'accuratezza dei dati è uno dei requisiti per la messa in commercio dei sistemi di IA ad alto rischio. È una specificità introdotta dall'art. 10 del Regolamento, che prevede al comma 3 che i set di dati utilizzati per l'addestramento dei modelli debbano essere «sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista»[64]. Nonostante ogni principio debba essere letto nello specifico contesto dove è inserito, è immediato il parallelismo con i principi applicabili al trattamento dei dati personali elencati all'art. 5 GDPR, dove si trovano, tra gli altri, il principio di minimizzazione, di esattezza, di integrità.

Privacy by design e *by default*: il Regolamento statuisce che i sistemi di IA, e, nello specifico, quelli che prevedono l'uso di dati per l'addestramento di modelli, debbano essere sviluppati considerando una molteplicità di elementi, tra cui: la raccolta di dati; le operazioni di trattamenti pertinenti ai fini della preparazione dei dati, compresi la pulizia dei dati, l'aggregazione, l'arricchimento; una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; l'individuazione di eventuali lacune o carenze nei dati e il modo con cui possono essere colmate. Il metodo prescelto dal Regolamento pare, quindi, ispirarsi ai principi di *privacy by design* e *by default* di cui all'art. 25 GDPR, che richiedono che ogni progetto avente ad oggetto dati personali sia pensato fin dalla sua ideazione secondo un'impostazione *privacy friendly*, ovvero minimizzando e calibrando i dati personali trattati strettamente necessari per il raggiungimento delle finalità del progetto stesso.

Principio di trasparenza: il Regolamento fissa specifici doveri di trasparenza, nella misura in cui prevede che i sistemi di intelligenza artificiale ad alto rischio debbano essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utilizzatori di interpretare l'output del sistema e utilizzarlo adeguatamente. Anche tale previsione sembra richiamare uno dei principi portanti del GDPR e, in particolare, il principio di trasparenza formalizzato dall'art. 5 del GDPR che mette in capo ai titolari del trattamento l'obbligo di rendere gli interessati consapevoli di come verranno trattati e successivamente conservati i dati personali in relazione allo specifico trattamento svolto, nonché dei rischi ad esso correlati. Quest'obbligo di trasparenza si concretizza nel rispetto dei doveri informativi di cui gli artt. 13 e 14 del GDPR che prevedono che il titolare – prima di avviare un trattamento di dati personali – fornisca ai relativi soggetti interessati un'idonea informativa privacy, tramite cui esporre le modalità con cui saranno trattati i dati personali raccolti.

Processi decisionali automatizzati: l'art. 22 del GDPR, che disciplina il trattamento di dati personali che avviene per mezzo di processi decisionali automatizzati, costituisce il maggior punto di contatto con l'AI Act, dal momento che tale disposizione normativa ha ad oggetto proprio fattispecie di trattamento, come la profilazione, effettuate con il ricorso all'intelligenza artificiale. Invero, giova notare come, mentre la logica perseguita dall'AI Act presuppone di *default* lo svolgimento di processi decisionali automatizzati – seppure controllati attraverso un'attenta sorveglianza umana – l'art. 22 del GDPR, *a contrario*, sancisce il diritto per gli interessati di non essere sottoposti ad una decisione basata unicamente sul trattamento automatizzato finalizzata all'assunzione di una decisione rilevante per la propria sfera giuridica. Ciononostante, l'art. 22 non fissa un divieto assoluto ma, tramite una clausola di apertura *ad hoc*, ammette un trattamento automatizzato di dati personali quando questo sia necessario all'esecuzione di un contratto di cui è parte l'interessato, quando sia autorizzato dal diritto dell'Unione, oppure quando vi sia il consenso dell'interessato stesso[65]. A tal proposito, è interessante notare come – nonostante sia il GDPR a prevedere un divieto relativo rispetto a trattamenti automatizzati di dati personali

64. Art. 10, par. 3, Regolamento Ue sull'intelligenza artificiale.

65. Per una disamina approfondita in materia si veda Napoli 2020, pp. 326-329.

che, tuttavia, non esclude aprioristicamente ma consente alle condizioni sopra menzionate – è però l'AI Act a vietare espressamente alcuni processi decisionali automatizzati (tra cui, a titolo esemplificativo, il *social scoring*) che, ai sensi della normativa privacy, sarebbero stati ammessi seppur con adeguate cautele e misure. In tal senso, è bene allora riflettere sulle ricadute che le incongruenze sopra delineate tra le due fonti normative potrebbero avere sul piano pratico, specialmente se si pensa ai contesti di lavoro aziendali, dove spesso esigenze di business portano a considerare progetti complessi e talvolta basati sull'uso dell'intelligenza artificiale.

Tirando le fila di quanto sopra analizzato, è possibile affermare che, nonostante le molteplici similitudini riscontrabili tra GDPR ed AI Act, resta essenziale focalizzarsi sull'assenza, allo stato attuale, di un meccanismo di raccordo procedurale adeguato tra le due discipline, che determina l'insorgere di almeno tre profili di criticità[66].

In primo luogo, si corre il rischio di imporre obblighi eccessivi agli attori privati, che dovranno quindi rileggere l'applicazione dell'art. 22 del GDPR alla luce del ben più ampio panorama dell'intelligenza artificiale.

In secondo luogo, senza idonee linee guida delle competenti autorità di controllo, gli operatori di mercato – sovente provenienti da sistemi giuridici diversi da quello europeo dove la protezione dei dati non è analogamente forte – saranno costretti ad espletare personalmente un bilanciamento tra gli interessi in gioco, giungendo a valutazioni arbitrarie e discrezionali. In tale contesto, forme di *self-regulation*[67], laddove esistenti, dovrebbero svolgere una mera funzione integrativa o complementare rispetto alla regolazione primaria[68], senza assorbire completamente i contenuti regolativi di quest'ultima, poiché diversamente s'incorrerebbe nel rischio che i pubblici poteri abdichino del tutto al compito essenziale di operare bilanciamenti tra valori, interessi e posizioni soggettive diverse[69].

In terzo luogo, la somma delle considerazioni precedenti, in aggiunta all'incertezza normativa, sortirebbe l'effetto di diminuire il raggio di tutela del singolo individuo[70]. Al riguardo, il fenomeno dell'*over-regulation*[71] è sempre un'arma a doppio taglio, nella misura in cui, se è vero che garantisce l'esistenza di più normative che da fronti diversi proteggono gli stessi diritti, dall'altro, se non ben regolato, rischia di ottenere l'effetto opposto alla finalità iniziale, mettendo a rischio quegli stessi diritti che si prefiggeva di tutelare.

3. Il sistema sanzionatorio dell'AI Act: luci ed ombre

Un altro profilo di necessaria comparazione tra le due normative in oggetto è rappresentato dal sistema sanzionatorio. A tal riguardo, si evidenzia che il Regolamento inaugura un sistema sanzionatorio fondato sul principio di diretta proporzionalità e modellato, dunque, in relazione alla gravità della violazione, nonché delle dimensioni e del fatturato dell'operatore che ha commesso la sanzione. Non a caso, infatti, le misure sanzionatorie introdotte dall'AI Act variano sia per intensità sia per tipologia della sanzione in ragione di una molteplicità di criteri di riferimento.

Più dettagliatamente, il Regolamento prevede sanzioni che – in linea con quanto già previsto nel GDPR – sono parametrate al fatturato annuo globale riferito all'esercizio finanziario precedente del soggetto giuridico cui la violazione è contestata. Nello specifico, sono previste sanzioni fino: (i) al 7% del fatturato o a 35 milioni di euro per la violazione delle norme in materia di pratiche vietate o di non conformità ai requisiti relativi alla qualità dei dati; (ii) al 3% o a 15 milioni di euro per la gran parte delle altre violazioni, ivi incluse quelle relative alle disposizioni in materia di *General-purpose AI models*; (iii) all' 1,5% del fatturato o a 7,5 milioni

66. Sul punto, si veda, *inter alia*, Faini 2020, pp. 90-91.
67. Parona 2020.
68. Concordemente, si veda De Minico 2020, pp. 16-17.
69. Stradella 2019, p. 8.
70. De Gregorio-Paolucci 2022.
71. Si veda al riguardo Raffiotta 2023.

di Euro per la violazione di obblighi informativi[72]. Spetterà, poi, ai singoli Stati Membri implementare e articolare la disciplina sanzionatoria di dettaglio a livello nazionale. A valle dell'ormai vicina approvazione formale del testo, l'AI Act sarà produttivo di effetti giuridici secondo tempistiche differenti. In particolare, le disposizioni aventi ad oggetto le sanzioni saranno pienamente in vigore dodici mesi dopo l'approvazione del Regolamento. Conseguentemente, nei prossimi mesi, sarà di primaria importanza per *deployer* ed utilizzatori di sistemi di intelligenza artificiale attuare i necessari presidi contrattuali e di *compliance* richiesti dal Regolamento in commento.

L'apparato sanzionatorio introdotto dal Regolamento rievoca, per natura e caratteristiche costitutive, quello posto in essere dal GDPR. Invero, quest'ultimo stabilisce un impianto sanzionatorio che, come l'AI Act, impattando fortemente sul fatturato dei soggetti coinvolti, comprende sanzioni amministrative pecuniarie diverse a seconda del tipo di violazione accertata e della previsione normativa violata. Più nello specifico, gli articoli 83 e 84 del GDPR regolano rispettivamente le condizioni generali per infliggere sanzioni amministrative pecuniarie e l'entità di tali sanzioni. Queste ultime raggiungono un importo fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni meno gravi; mentre, per le infrazioni più gravi, si giunge fino ad un ammontare pari a 20 milioni di euro o fino al 4% del fatturato mondiale annuo precedente, se superiore, per le imprese. Inoltre, anche l'AI Act, come il GDPR, attribuisce all'autorità di controllo competente il compito di infliggere e determinare l'ammontare delle sanzioni, valutando caso per caso l'*an* e il *quantum* in base alle circostanze concrete, tra cui l'entità della violazione, la sua durata e il dolo o la colpa dell'autore. Ancora una volta, con l'AI Act, il legislatore europeo, così come già fatto con il GDPR, lascia all'organo di controllo un ampio margine di discrezionalità entro cui muoversi per esercitare il proprio potere sanzionatorio. Se ne trae la considerazione che, giacché spesso l'uso di un sistema di intelligenza artificiale presuppone ed implica un trattamento di dati personali, sarà difficile per la futura autorità di controllo far coesistere e coordinare tra loro il regime sanzionatorio dell'AI Act con quello del GDPR. Tale situazione di incertezza normativa è ancora più chiara se si tiene in debita considerazione l'assenza di apposite previsioni atte a regolare il rapporto tra le due discipline sanzionatorie e la probabilità che possa essere individuata come autorità di controllo competente per la regolazione dell'intelligenza artificiale un organo diverso dall'Autorità Garante per la protezione dei dati personali.

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 non appare del tutto sufficiente a garantire un'applicazione efficace. L'esperienza del GDPR mostra che un eccessivo affidamento sull'*enforcement* delle autorità nazionali si espone al rischio di difformità applicative, a causa delle notevoli divergenze di risorse e prassi di intervento nei diversi Stati membri. 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. Infine, occorre segnalare che il Regolamento non contiene meccanismi di azione per gli individui o gruppi danneggiati, nemmeno nella forma di reclamo. L'assenza di tali previsioni, che avrebbero compensato i limiti dell'*enforcement* pubblico, risulta certamente criticabile, avendo come effetto anche il ridimensionamento del ruolo della società civile nello sviluppo affidabile dell'IA[73].

4. Il sistema di governance dell'AI Act: la delicata scelta di un'autorità di controllo nazionale per regolare l'intelligenza artificiale

Il Regolamento delinea un sistema di governance che è possibile definire congiuntamente come "multilivello" e "multistakeholder"[74]. Ciò in quanto i meccanismi di governance messi a punto dal Regolamento agiscono sia a livello europeo sia a

72. Art. 99, Regolamento Ue sull'intelligenza artificiale.

73. Contissa et al. 2021, pp. 31-33.

74. Sul tema della governance, cfr. Pajno et al. 2019, p. 219.

livello nazionale per singolo Stato Membro, coinvolgendo inoltre una pluralità di attori.

Con riferimento al livello Ue, il Regolamento istituisce il Comitato europeo per l'Intelligenza artificiale (*European Artificial Intelligence Board*), la cui composizione riflette la logica di cooperazione istituzionale tra autorità di controllo nazionali e autorità di riferimento Ue che caratterizza la maggior parte degli atti normativi europei[75]. Infatti, il Comitato sarà composto da un rappresentante dell'autorità di vigilanza nazionale per Stato Membro e dal Garante europeo per la protezione dei dati (*European Data Protection Supervisor* – EDPS), mentre la presidenza sarà affidata alla Commissione. Per quanto concerne i poteri del Comitato, il Regolamento prevede che il Board dovrà principalmente garantire la cooperazione tra le autorità nazionali e supportare l'attività della Commissione tramite l'emanazione di pareri, raccomandazioni e linee guida, con un ruolo, quindi, eminentemente consultivo[76]. Pur limitandosi all'emanazione di atti di *soft law*, il supporto del Board sarà, tuttavia, essenziale per garantire un corretto e adeguato svolgimento dei compiti attribuiti in questa delicata materia alla Commissione europea, tra cui giova ricordare anche la complessa attività di tenuta e controllo della sopra accennata banca dati europea sui sistemi di intelligenza artificiale ad alto rischio[77]. Tale banca dati – che sarà creata e gestita dalla Commissione in collaborazione con gli Stati Membri – conterrà tutte le informazioni relative ai sistemi di IA ad alto rischio destinati al mercato europeo che i *provider* saranno tenuti a comunicare, ed avrà la finalità di assicurare un regime di controllabilità e pubblicità della circolazione di tali prodotti all'interno dell'Ue[78].

All'interno della stessa Commissione, il Regolamento sancisce, inoltre, l'istituzione di un *AI Office*, che supervisionerà l'applicazione e il rispetto delle disposizioni dell'AI Act[79]. Accanto ad essi, saranno poi costituiti (i) un *Advisory Forum* composto da stakeholder rappresentativi di industria, società civile e accademia, con funzioni consultive[80] e (ii) un *Scientific Panel of independent experts*, che avrà il compito di supportare l'AI Office nell'attività di corretta attuazione delle previsioni del Regolamento, con particolare riferimento ai *General-purpose AI models*[81].

Spostando l'attenzione sul livello nazionale di governance, invece, gli Stati Membri saranno chiamati ad individuare almeno: (i) un'autorità "di notifica" responsabile di istituire e attuare le procedure necessarie per la valutazione e notifica degli organismi di valutazione della conformità dei sistemi ad alto rischio e per il loro monitoraggio; (ii) un'autorità di sorveglianza del mercato, con poteri investigativi e correttivi, tra cui anche quello di accedere ai dati personali in fase di elaborazione e alle informazioni necessarie per eseguire i loro compiti[82].

In Europa, il primo tentativo di dare attuazione alle previsioni in materia di governance dell'AI Act si è ha avuto di recente in Spagna, dove nel settembre 2023 è stata istituita l'*Agencia Española de Supervisión de Inteligencia Artificial* ("AESIA"), ovvero la prima autorità di controllo in materia di intelligenza artificiale in Europa[83]. Prevista come parte integrante della Strategia nazionale spagnola per l'intelligenza artificiale, l'istituzione dell'AESIA si pone in netto anticipo rispetto all'entrata in vigore dell'AI Act, collocando la Spagna in posizione di avanguardia nel panorama europeo. La natura dell'Agenzia riflette la scelta della Spagna di costituire una nuova autorità di vigilanza anziché assegnare tale ruolo ad un organo già esistente, alimentando così gli orientamenti e le attenzioni del dibattito dottrinale attualmente in corso sul tema. Secondo quanto si evince dalla lettura dello

75. Carantani 2024.
76. Artt. 65 e 66, Regolamento Ue sull'intelligenza artificiale.
77. Art. 71, Regolamento Ue sull'intelligenza artificiale.
78. Casonato-Marchetti 2021, pp. 434-435.
79. Art. 64, Regolamento Ue sull'intelligenza artificiale.
80. Art. 67, Regolamento Ue sull'intelligenza artificiale.
81. Art. 68, Regolamento Ue sull'intelligenza artificiale.
82. Capacci-Galli-Loreggia-Maroccia 2024, pp. 8-9.
83. Al riguardo, si veda Valdés Borruey-Latasa Vassallo-Ñíguez Olalla 2023.

Statuto dell'Agenzia – pubblicato sul *Boletín Oficial del Estado* all'interno del Real Decreto 729/2023 del 22 agosto – l'AESIA sarà responsabile dell'intera materia dell'intelligenza artificiale e, in particolare, della corretta implementazione del Regolamento europeo sull'IA. L'Agenzia avrà prevalentemente compiti di supervisione, consulenza, sensibilizzazione, formazione e finanche poteri ispettivi e sanzionatori. Quanto alla natura giuridica, l'Agenzia farà capo al Ministero degli Affari economici e della Trasformazione digitale, attraverso il Segretario di Stato sulla Digitalizzazione e Intelligenza Artificiale cui spetterà il ruolo di Presidente, e godrà di personalità giuridica pubblica, con patrimonio proprio e autonomia di gestione. In linea con quanto enunciato dal suo Statuto, l'AESIA eserciterà le proprie attività ispirandosi ai principi di interesse generale, autonomia, indipendenza tecnica e trasparenza, efficacia ed efficienza, cooperazione interistituzionale ed uguaglianza[84].

In Italia, la scelta in merito all'individuazione dell'autorità di controllo competente sembrerebbe ancora aperta. In tale contesto, infatti, è al momento in corso un vivace dibattito politico-istituzionale che vede su due posizioni differenti, da un lato, il Governo e, dall'altro, l'Autorità Garante per la protezione dei dati personali. In particolare, dal fronte dell'esecutivo, è stato approvato dal Consiglio dei Ministri del 23 aprile 2024 un disegno di legge «per l'introduzione di disposizioni e la delega al Governo in materia di intelligenza artificiale» che attribuisce le funzioni di supervisione e controllo richieste dall'AI Act all'Agenzia per l'Italia Digitale ("AgID") e quelle relative alla cybersecurity all'Agenzia per la cybersicurezza nazionale ("ACN"). La scelta di affidare ad AgID ed ACN – agenzie entrambe soggette alle funzioni di indirizzo e coordinamento della Presidenza del Consiglio – il potere di vigilanza in materia di intelligenza artificiale intende rispecchiare la vision strategica del Governo italiano incentrata sull'efficacia e l'efficienza nella governance dell'IA. Tali agenzie sono, in effetti, dotate di competenze complementari e altamente specializzate da considerarsi essenziali per affrontare le sfide poste dall'intelligenza artificiale in ambito di cittadinanza, industria, sicurezza, protezione dei dati e sicurezza nazionale. Di contro – ad avviso del Governo – la scelta di attribuire questo ruolo ad un'autorità amministrativa indipendente porterebbe con sé alcune difficoltà applicative, dal momento che le Authority potrebbero non avere quelle competenze tecniche e digitali, oltre che l'integrazione con il sistema digitale nazionale, già in possesso di AgID e ACN[85].

Dal canto suo, l'Autorità Garante per la protezione dei dati personali si è più volte espressa in ordine al sistema di governance delineato dall'AI Act[86], sottolineando l'importanza di individuare un'autorità autonoma e neutrale. In una segnalazione inviata ai Presidenti di Senato e Camera e al Presidente del Consiglio[87], l'Autorità ha ricordato che il Regolamento si fonda sull'articolo 16 del Trattato sul funzionamento dell'Unione europea – che è la base giuridica della normativa di protezione dei dati – e che lo stesso Regolamento prevede il controllo delle autorità di protezione dei dati personali su processi algoritmici che utilizzino dati personali. Conseguentemente, ha ribadito che siffatte autorità sono gli unici organi effettivamente destinatari di una riserva di competenza sancita dall'AI Act e, in quanto indipendenti, legittimate a svolgere le funzioni di controllo in settori delicati come quello delle attività di contrasto. Segnatamente, l'Autorità ha colto l'occasione per evidenziare nuovamente di essere in possesso di quei requisiti di competenza e indipendenza necessari per attuare il Regolamento con l'obiettivo di un livello elevato di tutela dei diritti fondamentali. Al riguardo, il Garante sottolinea che tale scelta avrebbe anche il merito di generare una semplificazione per gli utenti, che potrebbero così rivolgersi ad un'unica autorità per questioni inerenti a sistemi di intelligenza artificiale che trattino dati personali, senza il rischio di conflitti di competenza o di duplicazione di oneri amministrativi.

Come è evidente, l'attribuzione a livello nazionale del ruolo di autorità di controllo per l'intelligenza artificiale costituisce un *thema decidendum* assai complesso, articolato su una pluralità di posizioni e considerazioni non sempre inconciliabili.

84. Catanzano 2023.

85. Cfr. Anastasio 2024; Esperti 2024; Donatio 2024.

86. Garante per la protezione dei dati personali 2022.

87. Garante per la protezione dei dati personali 2024.

Ciò che emerge da un'analisi macroscopica della questione è la stringente necessità di dar vita ad una concreta alleanza di sistema tra soggetti con un ruolo neutro e di garanzia ma anche provvisti di consolidate strutture tecniche, nel solco, ovviamente, di un quadro normativo interno chiaro, sia in merito al riparto di competenze, sia in relazione agli ambiti di collaborazione. Solo attraverso un modello di intenso coordinamento tra competenze, sensibilità e strutture si potrà rimanere in linea con l'obiettivo di fondo della disciplina europea, ossia assicurare il funzionamento di strumenti di tutela giuridicamente effettivi, a tutela delle libertà degli utenti e in grado di promuovere il pieno sviluppo del mercato unico digitale.

5. Conclusioni

Come tutti gli strumenti normativi che si prefiggono l'obiettivo di essere *maxima summa* di un panorama complesso e frastagliato, così come quello delineato dall'intelligenza artificiale, anche l'AI Act non può essere esente da riflessioni e prospettive *de iure condendo*, strumentali ad una migliore interiorizzazione dei suoi contenuti.

In primo luogo, va evidenziato come l'impianto normativo in questione appaia inevitabilmente rigido. Invero, l'intenzione del legislatore europeo di mappare ogni possibile tipologia di sistema di intelligenza artificiale, categorizzata per livello di rischio, pur essendo lodevole dal punto di vista formale, in quanto volta a garantire esaustività dei contenuti e completezza della normazione, corre, tuttavia, il rischio di risultare nel breve periodo anacronistica e desueta. È un fatto che l'evoluzione della tecnica nel campo dei sistemi di intelligenza artificiale proceda incessantemente e a grande velocità: ciò comporta che, facilmente, le previsioni del Regolamento potrebbero non essere in linea con le tecnologie nel frattempo subentrate[88], per quanto la stessa classificazione dei sistemi di IA sarà soggetta a revisione periodica, come previsto dal Regolamento stesso. Quest'ultimo, come il GDPR, introduce un sistema giuridico fondato sulla gestione del rischio ma, a differenza del regolamento sulla protezione dei dati, non contempla l'applicazione del principio di *accountability*, in forza del quale il titolare del trattamento è tenuto ad applicare le disposizioni regolamentari in conformità alle caratteristiche proprie del trattamento di dati personali e dimostrare di aver adeguatamente attuato la *compliance* richiesta. Tale responsabilizzazione imposta dal GDPR al titolare del trattamento consente un costante adattamento del modello di gestione del rischio in grado di rendere sempre flessibile il dettato normativo. Al contrario, nell'AI Act questa tendenza si inverte ed è, quindi, lo stesso legislatore europeo che ha l'onere di individuare quali sistemi di intelligenza artificiale siano da considerare ad alto rischio e come tali rischi debbano essere mitigati. Conseguentemente, la staticità dell'approccio introdotto dal Regolamento pone come criticità quella di avere un sistema non abbastanza dinamico rispetto ai continui sviluppi dell'intelligenza artificiale.

In secondo luogo, va evidenziato che il Regolamento presenta un meccanismo di tutela dei diritti e delle libertà della persona molto più ristretto e contenuto rispetto a quello offerto dal GDPR. Infatti, mentre nel GDPR gli interessati hanno un'ampia gamma di diritti da poter esercitare nei confronti dei titolari del trattamento dei dati, in aggiunta agli strumenti delle segnalazioni e dei reclami da esercitare direttamente dinanzi alle autorità di controllo, nell'AI Act i rimedi riconosciuti agli interessati sono soltanto due. Da un lato, vi è la possibilità di presentare un reclamo dinanzi all'autorità di sorveglianza del mercato per violazioni del Regolamento e, dall'altro, è possibile esercitare, nei confronti del produttore di sistemi di IA ad alto rischio, il diritto a ricevere spiegazioni circa eventuali decisioni assunte sulla base dei risultati del sistema che incidano sui diritti e le libertà del soggetto istante. La mancanza di centralità dei diritti degli interessati e l'assenza di un regime di liability chiaro all'interno dell'AI Act lascia presumere, quindi, che – almeno per affinità di materia – il sistema di presidi sarà integrato dalle disposizioni su diritti, segnalazioni e reclami già previsti in materia di protezione dei dati personali.

Ulteriori criticità sorgono anche in relazione ai rinvii effettuati dal Regolamento al GDPR. In questo senso, infatti, nei punti in cui l'AI Act rinvia al GDPR sarebbe utile determinare in modo più chiaro i rapporti tra le due fonti regolatorie, assicurando un miglior coordinamento tra le diverse discipline. D'altro canto, nei casi in cui il

88. Cfr. Finocchiaro 2012.

Regolamento non rinvii espressamente al GDPR, si potrebbe essere indotti a pensare che sia ammissibile una deroga alla normativa sul trattamento dei dati personali[89].

In ultima analisi, va sottolineato come l'AI Act sia solo l'ultimo dei numerosi interventi normativi di questa legislatura europea sul mercato unico digitale.

Nella non facile opera di coordinamento[90] cui sarà chiamato il rinnovato legislatore europeo, sarebbero auspicabili alcune modifiche contestuali non solo al testo dell'AI Act ma anche a quello del GDPR, volte a migliorare il coordinamento e l'interrelazione tra le due discipline, in un'ottica di complessiva semplificazione del sistema.

In questa direzione, sembra parimenti auspicabile la predisposizione di un'opera di codificazione e coordinamento della pluralità delle fonti normative applicabili al settore del digitale[91], come strumento di prevenzione del rischio patologico di ipertrofia normativa[92].

Tale lavoro di riordino della materia appare di stringente urgenza, al fine di scongiurare il rischio che il legislatore europeo ha strenuamente cercato di evitare in questi ultimi anni, ossia rallentare il processo di digitalizzazione – proprio a causa della moltitudine di vincoli normativi incombenti sugli operatori di mercato – senza nemmeno innalzare il livello di tutela dei diritti dei cittadini dell'Unione[93]. In conclusione, la sistematizzazione della fitta trama normativa ad oggi esistente in Europa potrebbe rappresentare la via maestra da percorrere per orientare – senza frenare – lo sviluppo tecnologico[94], creando un ecosistema europeo aperto all'innovazione e concretamente in grado di sconfessare l'annoso leitmotiv «America innovates, China replicates, Europe regulates»[95].

Riferimenti bibliografici

S.A. Aaronson (2020), *America's uneven approach to AI and its consequences*, Working paper 2020-7, Institute for International Economic Policy Working Paper Series, George Washington University, April 2020

AA.VV. (2023), *L'Unione Europea approva l'AI Act*, Newsletter Bonelli Erede, 20 dicembre 2023

A. Alù (2023), *I differenti approcci regolatori in materia di intelligenza artificiale tra evoluzione tecnologica e risvolti applicativi*, in "Il Diritto di famiglia e delle persone", 2023, n. 3

P. Anastasio (2024), *Intelligenza Artificiale, ora è ufficiale: la vigilanza in Italia ad AgID e ACN*, in "Key-4Biz", 20 marzo 2024

AssoDPO (2023), *AI ACT, la meta è vicina: un nuovo standard globale*, 19 dicembre 2023

J. Black, A. Murray (2019), *The Regulatory Action – Regulating AI and Machine Learning: Setting the Regulatory Agenda*, in "European Journal of Law and Technology", vol. 10, 2019, n. 3

A. Bradford (2021), *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, Franco Angeli, 2021

F. Bravo (2021), *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in "Contratto e impresa Europa", 2021, n. 1

A. Burt (2021), *New AI Regulations Are Coming. Is Your Organization Ready?*, in "Harvard Business Review", April 30, 2021

89. Iacovelli-Fontana 2022, pp. 136-138.
90. In questo senso, cfr. Black-Murray 2019.
91. Contaldi 2021, p. 1213.
92. Torreggiani 2021.
93. In tal senso, Miniscalco 2020, p. 260.
94. Frosini 2022, p. 13.
95. Cfr., *inter alia*, Faralli 2019.

S. Calzolaio (2017), *Protezione dei dati personali*, in "Digesto delle Discipline Pubblicistiche. Aggiornamento VII", Utet, 2017

A. Capacci, G. Galli, A. Loreggia, I. Maroccia (2024), *Il nuovo regolamento europeo sull'IA: cosa cerca di fare e cosa fa*, in "Osservatorio sui Conti Pubblici Italiani", 22 febbraio 2024, pp. 8-9

I. Carantani (2024), *IA Act: l'Unione Europea approva la proposta di Regolamento sull'intelligenza artificiale*, in "Ius in itinere", 3 maggio 2024

C. Casonato, M. Fasan, S. Penasa (a cura di) (2022), *Diritto e Intelligenza Artificiale*, in "DPCE Online", 2022, n. 1

C. Casonato, B. Marchetti (2021), *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in "BioLaw Journal – Rivista di Bio Diritto", 2021, n. 3

L. Catanzano (2023), *Il Regno dell'Intelligenza Artificiale: la Spagna istituisce la prima agenzia statale di supervisione dell'IA in Europa*, in "Fondazione Leonardo – Civiltà delle Macchine", 11 ottobre 2023

C. Cath, S. Watcher, B. Mittelstadt, M. Taddeo, L. Floridi (2018), *Artificial intelligence and the "Good Society": the US, EU and UK approach*, in "Science and Engineering Ethics", 2018, n. 2

G. Cerrina Feroni (2023), *Intelligenza artificiale e ruolo della protezione dei dati personali*, 14 febbraio 2023

G. Cerrina Feroni (2022), *Luci e ombre della Data Strategy europea*, 13 maggio 2022

E. Chiti, B. Marchetti (2020), *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in "Rivista della Regolazione dei mercati", 2020, n. 1

C.A. Ciaralli (2023), *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, in "federalismi.it", 2023, n. 15

C. Colapietro, A. Moretti (2020), *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in "BioLaw Journal – Rivista di BioDiritto", 2020, n. 3

Commissione europea (2023), *Intelligenza artificiale – Domande e risposte*, 12 dicembre 2023

Commissione Europea(2015), *Agreement on Commission's EU data protection reform will boost Digital Single Market*, December 15, 2015

G. Contaldi (2021), *Intelligenza artificiale e dati personali*, in "Ordine internazionale e diritti umani", 2021, n. 5

G. Contissa, F. Galli, F. Godano, G. Sartor (2021), *Il Regolamento europeo sull'intelligenza artificiale: analisi informatico-giuridica*, in "i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2021, n. 2

G. De Gregorio, F. Paolucci (2022), *Dati personali e AI Act*, in "Media Laws. Law and Policy of the Media in a Comparative Perspective", April 15, 2022

G. De Minico (2023), *Relazione introduttiva*, in G. De Minico, M. Villone (a cura di), "Stato di diritto – Emergenza – Tecnologia", Consulta on line, 2020

I. Donatio (2024), *IA, Butti: presto Ddl, prevista Agenzia e non Autorità indipendente*, in "The Watcher Post", 12 marzo 2024

W.D. Eggers, R. Hamill, A. Ali (2013), *Data as currency. Government's role in facilitating the exchange*, in "Deloitte Review", 2013, n. 13, pp. 19-31

G. Esperti (2024), *Cosa sappiamo sulla strategia italiana sull'intelligenza artificiale*, in "Wired", 12 marzo 2024

F. Faini (2020), *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in "federalismi.it", 2020, n. 16

C. Faralli (2019), *Diritti e nuove tecnologie*, in "Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica", 2019, n. 2

G. Finocchiaro (2022), *La regolazione dell'intelligenza artificiale*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

G. Finocchiaro (2019), *Intelligenza Artificiale e protezione dei dati personali*, in "Giurisprudenza Italiana", 2019, n. 7

G. Finocchiaro (2012), *Riflessioni su diritto e tecnica*, in "Il diritto dell'informazione e dell'informatica", 2012, n. 4-5

G. Finocchiaro, O. Pollicino (2022), *La strategia europea sui dati e le divergenze con quella italiana*, in "Il Sole 24 ORE", agosto 2022

L. Floridi, J. Cowls (2019), *A unified framework of five principles for AI in society*, in "Harvard Data Science Review", vol. 1, 2019, n. 1

T.E. Frosini (2022), *L'orizzonte giuridico dell'intelligenza artificiale*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 1

Garante per la protezione dei dati personali (2024), *Segnalazione al Parlamento e al Governo sull'Autorità per l'I.A.*, 25 marzo 2024

Garante per la protezione dei dati personali (2022), *Memoria del Garante per la protezione dei dati personali – COM 2021(206) Proposta di regolamento (UE) sull'intelligenza artificiale*, Camera dei Deputati – Commissioni IX e X riunite, 9 marzo 2022

D. Iacovelli, M. Fontana (2022), *Nuove sfide della tecnologia e gestione dei rischi nella proposta di regolamento europeo sull'intelligenza artificiale: set di training, algoritmi e qualificazione dei dati. Profili critici*, in "Il diritto dell'economia", 2022, n. 3

A. Mantelero (2022), *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, vol. 36, Springer, 2022

A. Mantelero, D. Poletti (a cura di) (2018), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna, Studi in tema di Internet Ecosystem*, Pisa University Press, 2018

B. Marchetti, L. Parona (2022), *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in "DPCE Online", 2022, n. 1

N. Miniscalco (2020), *Il diritto alla protezione dei dati personali al tempo della mobilità intelligente*, in "Forum di Quaderni Costituzionali", 2020, n. 1

C. Napoli (2020), *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in "Rivista AIC", 2020, n. 3

C. Novelli (2024), *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in "federalismi.it", 2024, n. 2

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, 11 June 2019

F. Pacileo (2022), *L'intelligenza artificiale nel prisma dell'impresa: evoluzione normativa e prospettive di studio*, in "Annuario 2022. Osservatorio Giuridico sulla Innovazione Digitale", Sapienza Università Editrice, 2022

U. Pagallo (2017), *Intelligenza Artificiale e diritto. Linee guida per un oculato intervento normativo*, in "Sistemi intelligenti", 2017, n. 3, pp. 615-636

A. Pajno, M. Bassini, G. De Gregorio et al. (2019), *AI: profili giuridici Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 3

L. Parona (2020), *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, soft law e self-regulation*, in "Rivista della Regolazione dei mercati", 2020, n. 1

M.G. Peluso (2023), *Intelligenza artificiale e tutela dei dati. Prospettive critiche e possibili benefici per una governance efficace*, Giuffrè, 2023

O. Pollicino, M. Bassini (2017), *Art. 8. Protezione dei dati personali*, in R. Mastroianni, O. Pollicino, S. Allegrezza et al. (a cura di), "Carta dei diritti fondamentali dell'Unione europea", Giuffrè, 2017

E.C. Raffiotta (2023), *Dalla* self-regulation *alla* over-regulation *in ambito digitale: come (e perché) di un necessario cambio di prospettiva*, in "Osservatorio sulle Fonti", 2023, n. 2

G. Resta (2022), *Cosa c'è di "europeo" nella proposta di regolamento UE sull'intelligenza artificiale?*, in "Il Diritto dell'informazione e dell'informatica", 2022, n. 2

H. Roberts, J. Cowls, J. Morley et al. (2021), *The Chinese Approach to AI: An Analysis of Policy, Ethics, and Regulation*, in "AI and Society", vol. 36, 2021

M.U. Scherer (2016), *Regulating artificial intelligence systems: risks, challenges, competencies, and strategies*, in "Harvard Journal of Law & Technology", vol. 29, 2016, n. 2

E. Stradella (2019), *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in "MediaLaws. Rivista di diritto dei media", 2019, n. 1

S. Torreggiani (2021), *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in "Rivista italiana di informatica e diritto", 2021, n. 1

M. Valdés Borruey, L. M. Latasa Vassallo, M. Ñíguez Olalla (2023), *Spain: Agency for the supervision of AI – overview*, in "Data Guidance", November 2023

M. Veale, K. Matus, R. Gorwa (2023), *AI and Global Governance: Modalities, Rationales, Tensions*, in "Annual Review of Law and Social Science", 2023, n. 19

R. van den Hoven van Genderen (2017), *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in "European Data Protection Law Review", 2017, n. 3