Protezione dei dati personali tra *AI Act* e Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale. Spunti di riflessione

di *Roberto Lattanzi**

Nonostante la diversa natura che li caratterizza, la *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS 225) del Consiglio d'Europa e il regolamento dell'Unione europea sull'intelligenza artificiale (*AI Act*) hanno tra i propri obiettivi la protezione dei diritti fondamentali e, tra questi, il diritto alla riservatezza e alla protezione dei dati personali. Entrambi gli strumenti contengono, a tal fine, espresse clausole di salvaguardia rispetto all'applicazione delle discipline di protezione dei dati personali, anche in relazione ai trattamenti che possono essere effettuati lungo il "ciclo di vita" dei sistemi di IA.

Più in particolare, l'AI Act introduce nell'Unione europea un ulteriore strato regolatorio, che si aggiunge a quello proprio delle discipline di protezione dei dati personali, senza sostituirvisi. Esso presenta in parte caratteri originali, indispensabili per tener conto delle peculiarità dei sistemi di IA, e in parte mutua principi generali – ma non la disciplina di dettaglio – già presenti nelle discipline di protezione dei dati.

Ancorché, secondo il disegno del legislatore, l'AI Act sia destinato a operare in sinergia, secondo un rapporto di complementarità, con le discipline di protezione dei dati personali, permangono tuttavia difficoltà nella realizzazione di un armonico sistema di *governance*, sia a livello nazionale, in ragione delle scelte operate dalla legge 23 settembre 2025, n. 132, ritenute non conformi all'AI Act, sia a livello europeo.

1. Considerazioni introduttive e delimitazione dell'oggetto della trattazione

Per quanto interessa ai fini delle riflessioni che seguono – dedicate all'interazione tra la (recente) regolamentazione dei sistemi di intelligenza artificiale[1]

* Le considerazioni svolte, proprie dell'autore, non sono riferibili all'Istituzione presso la quale opera.

1. Il riferimento deve essere diretto (qui e, più in generale, nel presente contributo) ai soli sistemi (o modelli) di IA che comportano, in fase di progettazione (*design*), sviluppo (*development*) o uso (*deployment*), il trattamento di dati personali (*cfr.* *considerando* 10 AI Act); diversamente non vengono in considerazione profili di interazione con le discipline di protezione dei dati personali.

e quella (ormai consolidata) in materia di protezione dei dati personali[2] –, l'ampio e prolungato dibattito che ha accompagnato l'introduzione di strumenti vincolanti per disciplinare l'impiego dei sistemi di intelligenza artificiale (IA) ha trovato due punti di approdo particolarmente significativi: il primo è costituito dalla *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS 225) (di seguito: "Convenzione"), con l'importante precisazione che la stessa trascende il perimetro del Consiglio d'Europa, sia in ragione del processo che ha portato alla sua adozione, cui hanno preso parte Paesi che non sono parti contraenti del Consiglio[3], sia per l'apertura potenzialmente universale agli Stati che, indipendentemente dall'appartenenza al Consiglio d'Europa, intendano ratificarla; il secondo è costituito dal regolamento dell'Unione europea sull'intelligenza artificiale (*AI Act*)[4].

Grazie ad entrambi, si è superato l'approccio iniziale, volto a elaborare (e prediligere) strumenti (variamente denominati) di *soft law*[5], per perseguire traguardi più ambiziosi; gli obiettivi dichiarati dell'AI Act sono, infatti, quelli di «migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione» (art. 1 AI Act)[6].

---

2. In chiave preparatoria rispetto alle iniziative al tempo in essere presso il Consiglio d'Europa e l'Unione europea, ricognizioni dedicate alle interrelazioni con i profili di protezione dei dati personali si devono, rispettivamente, ad A. Mantelero, *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedie*s, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Strasburgo, 25 gennaio 2019, T-PD(2018)09Rev e a G. Sartor e F. Lagioia, *Study: The impact of the General Data Protection Regulation on artificial intelligence*, Parlamento europeo, 2020.

3. I lavori del *Committee on Artificial Intelligence* (CAI) – cui era stato rimesso il compito di elaborare un *draft* finalizzato all'adozione di uno strumento giuridicamente vincolante a livello internazionale (www.coe.int/en/web/artificial-intelligence/cai) –, sono stati preceduti dall'intensa azione realizzata dall'*Ad Hoc Committee on Artificial Intelligence* (CAHAI) (www.coe.int/en/web/artificial-intelligence/cahai), riunitosi per la prima volta dal 18 al 20 novembre 2019, al quale si deve (tra l'altro) il *Feasibility study on a legal framework on AI design, development and application based on CoE standards*, adottato dal CAHAI il 17 dicembre 2020: in merito, vds. I. Ben-Israel - J. Cerdio - A. Ema - L. Friedman - M. Ienca - A. Mantelero -E. Matania - C. Muller - H. Shiroyama - E. Vayena, *Towards Regulation of AI Systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law*, CAHAI, Consiglio d'Europa, dicembre 2020. Per una recente disamina della parabola che ha condotto alla Convenzione quadro e un'introduzione con riguardo ai lineamenti generali che la caratterizzano, si rinvia a M. Hernández Ramos, *The Difficult Road to the Framework Convention. Dilemmas and Strengths in the Regulation of Artificial Intelligence by the Council of Europe*, 17 *It. J. Public L.* 1242 (2025).

4. Ancorché inesatta (*cfr.* J. Ziller, *The Council of Europe Framework Convention on Artificial Intelligence vs. the EU Regulation: two quite different legal instruments*, in *Riv. interdisc. dir. amm. pubbl.*, 2024, pp. 202, 214), per ragioni di brevità e in ragione del suo uso comune, si utilizzerà nel testo la dizione "AI Act" per riferirsi al regolamento (UE) 2024/1689 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 rispetto al quale, senza che lo stesso non abbia ancora trovato integrale applicazione (*cfr.* art. 111), è già stata presentata, all'interno del *Digital package*, una proposta che mira a introdurre modifiche rilevanti non solo ai fini dell'opera di progressivo assestamento della complessiva cornice normativa in materia di IA, ma anche per le interrelazioni con la materia della protezione dei dati personali: tali modifiche sono veicolate anzitutto tramite la proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regg. (UE) 2024/1689 e (UE) 2018/1139 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (*Omnibus* digitale sull'IA), COM (2025) 836 def.: sulla proposta, il Parlamento europeo ha adottato la posizione comune il 26 marzo 2026, P10TA(2026)0098 – *Semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale* (*Omnibus* digitale sull'IA). Ma deve altresì essere presa in considerazione la proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regg. (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e le dirr. 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 per quanto riguarda la semplificazione del quadro legislativo nel settore digitale, e che abroga i regg. (UE) 2018/1807, (UE) 2019/1150 e (UE) 2022/868 e la dir. (UE) 2019/1024 (*Omnibus* digitale), COM (2025) 837, sulla uale non ci si sofferma, ma che contiene disposizioni che potrebbero avere un effetto riflesso sulla materia dell'IA (prima fra tutte la possibile rivisitazione della definizione di "dato personale").

5. Non è qui possibile elencarli: per rilevanza su scala globale, basti il riferimento alla OECD (OCSE) *Recommendation of the Council on Artificial Intelligence* del 2019 (OECD/LEGAL/0449) e all'UNESCO *Recommendation on the Ethics of Artificial Intelligence*, 23 novembre 2021: per un loro primo (generale) confronto con la Convenzione quadro e l'AI Act, vds. Z. Turbék, *The Principle of Fairness in International AI Law in the Making*, in M. Varju e K. Mezei (a cura di), *The Challenges of Artificial Intelligence for Law in Europe*, Cham, 2025, pp. 45 ss.

6. Disposizione che si radica nei principi formulati dall'*High-Level Expert Group on AI* (HLEG-AI) per promuovere la diffusione di un'intelligenza artificiale "antropocentrica e affidabile" (*trustworthy*); così i contenuti delle *Ethics Guidelines for Trustworthy Artificial Intelligence* del 2019 (https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai) sono ripresi nel *considerando* n. 27 dell'AI Act che, anticipando i contenuti della parte dispositiva, così li sintetizza: «I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e *governance* dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità».

Al netto della dimensione di mercato, che non rientra (in via diretta) nella missione istituzionale del Consiglio d'Europa, le predette finalità sono assai prossime a quelle perseguite dalla Convenzione che, pur risentendo dell'*imprinting* dell'AI Act (ma fortemente ibridato da componenti emerse nel corso della negoziazione)[7], è espressamente preordinata alla tutela dei diritti fondamentali, dello Stato di diritto e dell'ordinamento democratico (vds. art. 1, comma 1, e art. 4) a fronte dei rischi (anche sistemici) che possono nascere dall'utilizzo delle (varie) tecnologie sottese alla locuzione "intelligenza artificiale", in ragione delle peculiari caratteristiche che le connotano[8].

Negoziati in parallelo e portati a termine a pochi mesi di distanza l'uno dall'altro[9] – con la Commissione europea incaricata di negoziare la Convenzione nell'interesse degli Stati membri (che sono in pari tempo Parti del Consiglio d'Europa) e, così, assicurarne la compatibilità con l'AI Act[10] –, i due strumenti si differenziano anzitutto per natura (sulla quale non è necessario qui insistere)[11], il che si riflette sulla struttura e sui contenuti che li caratterizzano. Significativamente diverso, infatti, è il livello di dettaglio delle disposizioni negli stessi contenute: a maglie (assai) larghe quelle presenti nella Convenzione, destinate a essere declinate nei vari ordinamenti tenendo conto delle rispettive tradizioni giuridiche[12], oltre che delle priorità fissate dalle diverse agende politiche; ben più strette quelle del regolamento, prioritariamente orientato al funzionamento del mercato interno e all'edificazione di uno strumentario volto, nelle intenzioni, ad assicurare l'*enforcement* della complessiva cornice regolatoria in materia di IA all'interno dell'Unione[13]. Caratteristiche che hanno indotto i primi commentatori a vedere nella Convenzione un primo nucleo di aggregazione di principi condivisi

7. Si pensi anzitutto all'art. 3, par. 1, lett. *b* della Convenzione, con riguardo al suo ambito di applicazione, ma anche agli strumenti, non normativi, per dare alla stessa attuazione.

8. La letteratura al riguardo è sterminata: vds. per tutti lo studio classico di S. Russell e Peter Norvig, *Artificial Intelligence. A Modern Approach*, Pearson, 2020, che (al par. 1.5), al di là dei rischi correlati all'impiego delle cd. armi autonome, alla cybersicurezza, alle infrastrutture critiche e alla disoccupazione di larghe fasce della popolazione, menziona quelli correlati alla sorveglianza (di massa) e alla capacità persuasiva propria dei sistemi di IA. Con riguardo ai profili di rischio rilevanti per le presenti riflessioni connessi ai più recenti sviluppi della cd. IA generativa, vds. I. Barberá e M. Popa-Fabre, *Privacy and Data Protection Risks in Large Language Models (LLMs)*, Expert Report on Privacy and Data Protection Risks in Large Language Models (LLMs), 48th Plenary meeting, 17 June 2025 (e, *ivi*, ulteriori riferimenti).

9. Merita ricordare le principali tappe che hanno caratterizzato il percorso dell'AI Act e della Convenzione: rispetto alla proposta di regolamento sull'intelligenza artificiale, COM(2021) 206 *final*, presentata il 21 aprile 2021: l'accordo politico è stato raggiunto, a seguito di plurime negoziazioni di trilogo, il 9 dicembre 2023 (con pubblicazione del testo dell'accordo provvisorio avvenuta il 2 febbraio 2024 e quindi del regolamento (UE) 2024/1689 del 13 giugno 2024, nella GUUE del successivo 12 luglio 2024). Per contro, i lavori sulla Convenzione hanno avuto inizio con la prima riunione del Comitato sull'IA (CAI), del 4-6 aprile 2022, e il testo, licenziato dal Comitato il 14 marzo 2024, è stato adottato il successivo 17 maggio dal Comitato dei ministri del Consiglio d'Europa per poi essere aperto alla firma in occasione della Conferenza dei ministri della giustizia tenutasi a Vilnius il 5 settembre 2024.

10. Terminato il processo di ratifica della Convenzione – rispetto al quale, l'11 marzo 2026, il Parlamento europeo ha adottato la risoluzione legislativa a favore del progetto di decisione del Consiglio relativa alla conclusione, a nome dell'Unione europea, della convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto, COM(2025) 265 *final* –, l'AI Act rappresenterà infatti lo strumento, comune agli Stati membri dell'UE, mediante il quale questi ultimi assicureranno la conformità degli ordinamenti nazionali alla Convenzione. Il mandato negoziale conferito alla Commissione europea mirava a prevenire disallineamenti del diritto dell'Unione rispetto a quello convenzionale, anche se in letteratura si sono già fatte rilevare alcune differenze, la più rilevante delle quali è il più ampio ambito di applicazione della Convenzione: i principi di quest'ultima si estendono a tutti i sistemi di IA, mentre l'AI Act lascia alcuni vuoti regolatori rispetto ai sistemi di IA che sfuggono alla tipizzazione dei rischi nello stesso contenuta – in particolare in relazione ai sistemi che, non annoverati tra quelli vietati (art. 5), sono considerati ad alto rischio (art. 6) o a rischio limitato (art. 50) – o, ancora, rientrano tra i modelli con finalità generale ovvero tra i modelli di IA per finalità generali con rischio sistemico (disciplinati, rispettivamente, agli artt. 53 e 55 AI Act). In questa prospettiva, secondo L. Cotino Hueso, *The Council of Europe's Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, in CERIDAP, n. 3/2024, pp. 53, 58, tali sistemi potrebbero dover essere in qualche modo presidiati dalle misure (pur assai generali) contenute nella Convenzione sull'IA.

11. Mentre l'AI Act trova diretta applicazione, secondo la scansione temporale stabilita dal menzionato art. 111 – suscettibile di essere modificata in caso di approvazione dell'*Omnibus* digitale sull'IA –, la Convenzione richiede invece in capo agli Stati che la ratificheranno l'approntamento di misure, non necessariamente di carattere normativo (*cfr.* art. 1, par. 2, nonché artt. 4 e 5), volte ad assicurare la tutela dei diritti fondamentali tenendo conto delle caratteristiche peculiari delle tecnologie riconducibili sotto l'ombrello della nozione di «intelligenza artificiale» accolta nel suo art. 2.

12. *Cfr.* art. 11.

13. Profilo anche questo analiticamente delineato nell'AI Act – sul quale sia consentito rinviare, anche per ulteriori richiami e rilievi critici, a R. Lattanzi, *AI Act e autorità di protezione dei dati personali*, in O. Pollicino - F. Donati - G. Finocchiaro - F. Paolucci (a cura di), *La disciplina dell'Intelligenza artificiale*, Giuffrè, Milano, 2025, pp. 367, 382 ss. – e appena abbozzato, invece, nella Convenzione (art. 14, part. parr. 1 e 2, lett. *c*).

sulla scena internazionale[14] e un possibile modello di riferimento su scala globale[15], ovvero anche solo un ponte tra lo *standard* di protezione offerto dall'Unione europea (al momento, probabilmente, tra i più elevati nel panorama internazionale) e quello presente in contesti nei quali un approccio più "liberale" può schiudere le porte a conseguenze pregiudizievoli, anche rilevanti, non solo per i diritti e le libertà individuali (e di gruppo), ma anche rispetto a interessi generali, mettendo finanche a repentaglio la democraticità degli ordinamenti (come già in qualche occasione l'esperienza ha lasciato intravedere)[16] e lo Stato di diritto.

2. I sistemi di IA e la necessità di un ulteriore strato regolatorio: oltre la protezione dei dati personali...

Senza poter indulgere a una più ravvicinata valutazione comparata dei due atti normativi, per quanto interessa ai nostri fini, merita evidenziare anzitutto un dato di fondo che li accomuna: entrambi si emancipano rispetto alle discipline e, prima ancora, ai modelli regolatori esistenti in materia di protezione dei dati personali, ancorché la possibilità di ricorrere a un "aggiornamento" di questi ultimi, per tener conto degli effetti dell'IA, si fosse palesata durante l'*iter* che ha condotto alla loro adozione.

Ciò accadde in modo manifesto in relazione alla Convenzione, atteso che, tra le opzioni regolatorie prefigurate dal CAHAI nel menzionato studio di fattibilità, faceva capolino anche una "modernizzazione" degli strumenti esistenti, e tra questi la cd. Convenzione "108+"[17].

Analogamente, in ambito unionale, nonostante l'approvazione avvenuta 14 marzo 2017 di una risoluzione sulle implicazioni dei *Big Data*[18] – prevalentemente incentrata sulla dimensione informazionale dell'IA (fortemente influenzata dai pareri resi dal Garante europeo della protezione dei dati)[19] –, sarà la (di poco precedente) risoluzione del 16 febbraio 2017, recante (le più generali) raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica[20], a giocare un ruolo determinante nell'innescare il processo che, considerata la cornice di riferimento

14. *Cfr*. O. Tambou, *La Convention-Cadre du Conseil de l'Europe sur l'IA: premier traité international encadrant les risques de l'IA sur les droits de l'homme, la démocratie et l'Etat de droit, à la valeur ajoutée incertaine*, in O. Tambou e M. Sweeney, *Le règlement européen sur l'IA et au delà: Quel encadrement de l'IA ?*, Bruylant, Bruxelles, 2025, pp. 293, 295: «Il s'agit d'un instrument flexible pouvant être complété par d'autres textes contraignants ou non soit pour approfondir certains de ses aspects, soit pour aborder l'utilisation de l'IA dans des secteurs spécifiques. L'ambition de la Convention est donc de dresser un premier cadre juridique commun acceptable par tous et d'ancrer juridiquement certains points sur lesquels un consensus émerge à l'échelle internationale».

15. Per Ziller, *The Council of Europe Framework Convention*, *op. cit*., p. 213, «the two main reasons for drafting a CoE treaty on artificial intelligence were to have a common text for all European States, including the UK after Brexit, and to participate in the global race to be the first to adopt a regulation on artificial intelligence, in the hope of serving as a model at least for pluralistic democracies». (...) «An additional reason was obviously to try to propose a text that could be adopted by a large number of other States, including the United States of America». A quest'ultimo proposito, merita ricordare che, sotto l'Amministrazione Biden, era stato inizialmente adottato, nel settore federale, l'*Executive Order* 14110, del 30 ottobre 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, revocato però all'atto dell'insediamento dell'Amministrazione Trump con l'*Executive Order* 14148, del 20 gennaio 2025, *Initial Rescissions of Harmful Executive Orders and Actions*, *Federal Register*, vol. 90, n. 17, 28 gennaio 2025 (Presidential Documents, 8237).

16. Vds. già V. Boehme-Neßler, *Big Data und Demokratie – Warum Demokratie ohne Datenschutz nicht funktioniert*, in *DVBl*, 2015, p. 1282; N. Witzleb e M. Park, *Big data, political campaigning and the law: democracy and privacy in the age of micro-targeting*, Abingdon, Oxon, Routledge, 2020; P. Richter, *Datenschutz und Demokratie - Microtargeting im Wahlkampf*, in A. Hentschel - G. Hornung - S. Jandt, *Mensch - Technik - Umwelt: Verantwortung für eine sozialverträgliche Zukunft, Festschrift für Alexander Roßnagel zum 70. Geburtstag*, Nomos, Baden-Baden, 2020, p. 303; in tempi più recenti, con riguardo all'annullamento delle elezioni in Romania, *cfr*. A. Verteş-Olteanu e D.A. Cărămidariu, *Safeguarding democracy: constitutional insights from Romania's election annulment*, in *DPCE*, 1/2025, p. 150.

17. *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, CM/Inf(2018)15-final - 128th Session of the Committee of Ministers (Elsinore, Danimarca, 17-18 maggio 2018). La soluzione cui si fa riferimento nel testo, per vero solo timidamente prospettata dallo stesso CAHAI sull'assunto essa non sarebbe stata in grado di «capture all concerns in relation to AI systems, given its (current) specific focus on the protection of individuals, and the processing of personal data» (*cfr*. CAHAI, *Feasibility Study*, cit. in nota 3, pt. 130 ss., 132), è tramontata con l'istituzione del CAI (e i *Terms of reference* dello stesso).

18. Risoluzione del 14 marzo 2017 sulle implicazioni dei *Big Data* per i diritti fondamentali: *privacy*, protezione dei dati, non discriminazione, sicurezza e attività di contrasto (2016/2225(INI)).

19. Al tempo, Giovanni Buttarelli: *cfr*. il parere n. 7/2015, del 19 novembre 2015, *Meeting the challenges of big data — A call for transparency, user control, data protection by design and accountability*, e il parere n. 8/2016, del 23 settembre 2016, *Opinion on coherent enforcement of fundamental rights in the age of big data*.

20. 2015/2103(INL), in *GUUE*, 18 luglio 2018, C 252/239. La risoluzione in parola, infatti, prendendo in considerazione lo spettro assai ampio delle applicazioni della robotica, anzitutto, e (anche se in misura più circoscritta, in ragione delle più ridotte applicazioni al tempo disponibili) dell'intelligenza artificiale, mirava a dar conto del più esteso impatto dell'introduzione dell'IA sulle varie dimensioni del vivere sociale (e, quindi, delle più ampie ricadute su molteplici settori dell'ordinamento giuridico), senza "appiattirsi" sulla sola (o prevalente) dimensione della protezione dei dati personali, la cui cornice regolatoria, peraltro, era stata al tempo da poco rinnovata: come si ricorderà,

fornita dal Libro bianco su «*Artificial Intelligence: A European Approach to Excellence and Trust*»[21], troverà compimento con l'AI Act[22]; questo spiega il diverso paradigma regolatorio (risultato "vincente") che caratterizza quest'ultimo, costituito dalle discipline relative alla sicurezza dei prodotti[23] e dei dispositivi medici[24], e il loro ancoraggio al cd. "*New Legislative Framework*"[25].

E tuttavia, se con l'AI Act si è inteso prendere le distanze dal modello regolatorio proprio delle discipline di protezione dei dati[26] – improntato alla neutralità tecnologica e fondato sull'attribuzione di diritti agli interessati e su un *set* di principi (espressi con la tecnica della norma e della clausola generale)[27] –, le sue diverse caratteristiche non devono però essere sopravvalutate. Infatti, pur utilizzando una diversa tecnica normativa, l'AI Act rimane comunque radicato sulla (e orientato alla) tutela dei diritti fondamentali[28] attraverso l'introduzione di (graduate) misure di protezione, sia nella fase di progettazione e sviluppo dei sistemi di IA, in particolare per quelli considerati ad alto rischio[29], sia, successivamente, durante l'uso[30]. E del resto, come reso ancor più evidente dal passaggio dalla cd. "*narrow AI*" alla "*general purpose AI*" (e come sta emergendo dall'insieme di applicazioni in grado di incidere significativamente su diritti fondamentali

sia il RGPD che la direttiva (UE) 2016/680, 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 (di seguito: "LED"), che ancora non trovavano applicazione, erano state adottate il 27 aprile 2016 (e quindi del tutto improbabile sarebbe stata una loro immediata rivisitazione). In ragione di questo più ampio approccio, non a caso la proposta di regolamento sull'intelligenza artificiale, del 21 aprile 2021, COM(2021) 206 *final*, sarebbe stata di lì a poco affiancata dalla proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale, 28 settembre 2022, COM(2022) 496 *final*, infine non adottata.

21. COM(2020) 65 *final*.

22. Al riguardo si rinvia, per un'analisi di maggior dettaglio e per ulteriori riferimenti, a Lattanzi, *AI Act e autorità di protezione dei dati personali*, *op. cit.*, pp. 391 ss.

23. *Cfr.* reg. (UE) 2023/988, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il reg. (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la dir. (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la dir. 2001/95/CE del Parlamento europeo e del Consiglio e la dir. 87/357/CEE del Consiglio.

24. *Cfr.* reg. (UE) 2017/745, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la dir. 2001/83/CE, i regg. (CE) n. 178/2002 e (CE) n. 1223/2009, e che abroga le dirr. 90/385/CEE e 93/42/CEE del Consiglio. Le opzioni seguite dalla Commissione europea con la proposta del 2021 rispecchiano le linee tracciate nella comunicazione *L'intelligenza artificiale per l'Europa*, 25 aprile 2018, COM(2018) 237 *final*, e chiaramente emergono dal Commission Staff Working Document *Liability for emerging digital technologies*, [Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe {COM(2018) 237 final}, 25.4.2018 SWD(2018) 137 *final*]: «*Emerging digital technologies, such as IoT, AI-powered advanced robots and autonomous self-learning systems, must meet the essential health and safety requirements laid down in the applicable EU safety legislation which ensures a single market for a wide range of equipment and machines* (...)».
Come è stato rilevato [*cfr.* M. Gornet, W. Maxwell, *The European approach to regulating AI through technical standards*, *Internet Pol'y Rev.* 13(3), 1, 2 (2024)], il Regolamento sull'IA si differenzia anche dagli ulteriori recenti interventi normativi dell'Unione nel contesto digitale, quali il *Data Governance Act* (reg. 2022/868), il *Data Act* (reg. 2023/2854), il *Digital Markets Act* (reg. 2022/1925) e il *Digital Services Act* (reg. 2022/2065).

25. Per una più ampia trattazione si rinvia a M. Veale e F. Zuiderveen Borgesius, *Demystifying the draft EU Artificial Intelligence Act: analysing the good the bad, and the unclear elements of the proposed approach*, in *Computer L. Rev. Int'l*, 2021(4), 97; vds. altresì G. Mazzini e S. Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. Camardi (a cura di), *La via europea per l'Intelligenza artificiale*, CEDAM (WK), Milano, 2023, pp. 21, 26 ss.

26. Come si è visto, processo simile ha caratterizzato anche la Convenzione, i cui contenuti, come si è anticipato, sono ben più sfumati in ragione del ben più alto livello di generalizzazione dei precetti nella stessa contenuta. Per questa ragione, il seguito della trattazione dedicata alle aree di sovrapposizione tra le discipline sui sistemi di IA e quelle di protezione dei dati personali si incentrerà sul diritto dell'Unione europea e i pertinenti riflessi nazionali (per quanto ci riguarda, in particolare, con la legge 23 settembre 2025, n. 132, «*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*»).

27. In prima battuta, quelli (*core*) contenuti nell'art. 5 del RGPD: è questa tecnica normativa che ha loro assicurato longevità e adattabilità al mutamento tecnologico (anche grazie all'opera delle autorità di protezione dei dati, ora riunite nel Comitato europeo per la protezione dei dati, in particolare mediante l'adozione di linee guida negli ambiti più disparati).

28. Così, condivisibilmente, L. Floridi, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, in *Philosophy and Technology*, 2021, pp. 215, 218: «From an ethical perspective, the AIA inherits the same foundational approach seen in the GDPR: it is based on protecting human dignity and fundamental rights. This is a very positive feature, even if the current proposal of the AIA seems to be somewhat more top-down, less flexible, and less focused on the protection of citizens and their rights than the GDPR».

29. Vds. il capo III dell'AI Act.

30. Si pensi alla sorveglianza umana (in varie forme) prevista, per i sistemi ad alto rischio, all'art. 14 AI Act.

dei singoli e su interessi generali[31] nonché dalle vulnerabilità che vanno palesandosi, talora singolari[32]), la lettura che vorrebbe ridurre i sistemi di IA a (semplice) "prodotto" – soggetto a "circolazione" sul mercato con l'apposizione del marchio CE[33] – rischia di rivelarsi, se non distorta, quantomeno semplificante: illuminante, al riguardo, la provocatoria affermazione secondo la quale «AI is not a dishwasher but a technology that poses risks to fundamental rights and democratic values, which transcend market regulation and consumer law»[34].

3. … ma non indipendentemente dalle discipline di protezione dei dati personali

In questa prospettiva, venendo più da vicino alla trattazione dei profili di protezione dei dati personali (e dei diritti fondamentali che per il tramite delle relative discipline possono venire in gioco ed essere tutelati)[35], va trovata allora la corretta chiave di lettura sottesa all'AI Act[36]. Tale operazione ricostruttiva deve essere effettuata sulla scorta di un saldo ancoraggio al dato normativo – interpretato e applicato alla luce dell'insieme dei valori presenti nella Carta dei diritti fondamentali dell'Unione europea e nelle tradizioni costituzionali comuni degli Stati membri – e, per quanto ciò possa presentare "passaggi" non semplici, lascia intravedere uno spazio di reciproca integrazione tra la disciplina in materia di IA e quelle di protezione dei dati personali[37], anche alla luce dell'articolato meccanismo di *governance* prefigurato dall'AI Act e integrato a livello nazionale[38].

Il fondamento di questa chiave di lettura va rinvenuto nella circostanza che non solo tra gli obiettivi dell'AI Act, come si è detto, vi è quello di preservare (tra gli altri diritti fondamentali) i valori della riservatezza e della protezione dei dati personali[39], ma pure che, anche per perseguire tale obiettivo, vengono espressamente fatte salve (in quanto applicabili) le discipline di protezione dei dati personali[40]: in questo senso si esprimono più disposizioni all'interno dell'AI Act, a partire dall'art. 2, par. 7[41].

Il significato e l'effetto di questa "clausola di salvaguardia" – nella materia in esame, davvero non riducibile a clausola di stile – è quello di riconoscere e rendere evidente che le tecniche di tutela contenute nel nuovo silos regolatorio dedicato all'IA[42] – che pur contiene misure innovative rispetto a quelle che

31. *Cfr*., da ultimo, la vicenda che ha interessato Grok in relazione alla diffusione di contenuti illegali, quali immagini sessualmente esplicite oggetto di manipolazione e contenuti che potrebbero costituire materiale pedopornografico, che forma oggetto di investigazione da parte della Commissione europea (https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_203/IP_26_203_EN.pdf). In materia vds., per primi riferimenti, V. Baines, *Emerging technologies: threats and opportunities for the protection of children against sexual exploitation and sexual abuse*, Background paper for the Lanzarote Committee, 2024.

32. *Cfr*. lo studio recente di P. Bisconti *et al*., *From Adversarial Poetry to Adversarial Tales: An Interpretability Research Agenda*, in *arXiv*:2601.08837v2 [cs.CL], 16 gennaio 2026.

33. *Cfr*. art. 48 AI Act.

34. F. Palmiotto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation*, in *Eur. J. Risk Regulation*, vol. 16, n. 2/2025, pp. 770, 777.

35. È opportuno ricordare che, in base all'art. 1, par 2, reg. (UE) 2016/679, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la dir. 95/46/CE (regolamento generale sulla protezione dei dati, di seguito "RGPD"), lo stesso «protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali».

36. Tenendo a mente il dato di realtà costituito da tecnologie e connesse applicazioni in costante evoluzione e, in pari tempo, le mutevoli vulnerabilità e rischi (talora sistemici) che le stesse presentano.

37. Vds., per gli sviluppi, *infra*, par. 4.

38. Al riguardo, *infra*, par. 5.

39. *Cfr*. i *considerando* nn. 10, 48 e 69 dell'AI Act.

40. Le presenti riflessioni si incentrano prevalentemente sul RGPD e non si estendono alle restanti discipline di protezione dei dati personali (LED e reg. (UE) 2018/1725), né alla direttiva 2002/58/CE, cui è rimessa la tutela della vita privata e della riservatezza delle comunicazioni, «in particolare stabilendo le condizioni per l'archiviazione di dati personali e non personali e l'accesso ai dati in apparecchi terminali», profilo espressamente menzionato al *considerando* n. 10 dell'AI Act e potenzialmente rilevante (anzitutto) per l'addestramento dei sistemi di IA.

41. Vds. anche il *considerando* n. 10 AI Act. Nello stesso senso depongono anche ulteriori indici normativi presenti nell'AI Act: ancorché in relazione ad altro profilo (di seguito trattato al punto 4.2), vds. la previsione contenuta nell'art. 10, par. 5, AI Act, nonché l'art. 28, par. 10. A non diversa conclusione si perviene anche guardando alla Convenzione: seppure con *wording* più elastico (volto ad includere «*privacy and personal data protection*») e con un più elevato livello di generalizzazione, nello stesso senso si esprime infatti il suo art. 11.

42. Più precisamente, mentre l'AI Act per sé assume valore regolatorio, ciò accadrà solo a seguito dell'adozione di misure specifiche (non necessariamente di natura normativa) con riguardo alla cornice regolatoria prevista dalla Convenzione quadro.

caratterizzano le discipline di protezione dei dati, misure indispensabili per prevenire distorsioni (se non discriminazioni) nell'impiego di sistemi che si fondano su una logica probabilistica[43] e non deterministica[44] – si aggiungono a quelle esistenti, non le sostituiscono: un livello adeguato di tutela dei beni che l'AI Act intende perseguire si può raggiungere quindi (come è ragionevole) opportunamente integrando, in chiave evolutiva[45], le garanzie esistenti con quelle nuove, mediante interventi correttivi/integrativi, nella misura necessaria, e con l'applicazione congiunta, per quanto possibile armonica[46], del sistema di regole contenute in entrambe le discipline.

Con l'ulteriore precisazione che, siccome talune regole rimontano a principi condivisi, si rende necessario, da un lato, prevenire un'inutile ridondanza negli adempimenti (in particolare, da parte dei *provider* e dei *deployer* dei sistemi di IA) e, dall'altro, si dovrebbe stabilire, nel pieno rispetto dell'AI Act e delle discipline di protezione dei dati (per quanto qui interessa)[47], un efficace sistema di *governance* da parte dei soggetti istituzionali chiamati a svolgere funzioni di controllo.

4. AI Act e discipline di protezione dei dati personali: una necessaria (ma non sempre agevole) complementarità

Con l'AI Act si è, come detto, aggiunto uno strato regolatorio ulteriore rispetto a quello offerto dalle sole discipline di protezione dei dati personali in caso di loro trattamento all'interno del ciclo di vita dei sistemi di IA. Esso dovrebbe consentire di minimizzare i rischi per i valori (individuali e collettivi) che l'Unione europea intende proteggere, grazie all'introduzione di misure appropriate fondate su un (consapevole e corretto) approccio basato sul rischio[48]. Siffatte misure sono (almeno in parte) originali rispetto a quelle proprie delle discipline di protezione dei dati e prevedono che i principali attori, alla luce del rispettivo ruolo (anzitutto quello di

43. E, per questa ragione, suscettibili di determinare (o ingenerare) distorsioni (*bias*), nel caso in cui i *data set* utilizzati in fase di sviluppo non posseggano le proprietà statistiche appropriate, considerate le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato (*cfr. considerando* n. 67 e art. 10, par. 2, lett. *f*, dell'AI Act). Beninteso, ciò non significa che sistemi deterministici, per ciò solo, non corrano essi stessi il rischio di produrre distorsioni o discriminazioni, ben potendo l'algoritmo (finanche decisionale) utilizzato essere espressamente progettato per discriminare (illecitamente) singoli o classi di individui.

44. Si pensi, anzitutto, alle pratiche di *governance* e gestione dei *data set* di addestramento, convalida e prova dei sistemi di IA ad alto rischio individuate all'art. 10, par. 2-5 dell'AI Act (sul quale si tornerà nel testo), che trascendono, in ragione delle peculiarità dei sistemi in esame, le misure contenute nelle discipline di protezione dei dati, e, non diversamente, le misure volte ad assicurare un livello di tracciabilità del funzionamento dei sistemi di IA ad alto rischio (art. 12 del regolamento).

45. *Cfr.* S. Wachter, *Data protection in the age of Big Data - Europe's data protection laws must evolve to guard against pervasive inferential analytics in nascent digital technologies such as edge computing*, in *Nature Electronics*, vol. 2, n. 6-7/2019.

46. Che tale coordinamento non possa darsi per scontato si desume già dal tenore di alcune modifiche normative che si intendono introdurre con il *digital omnibus package*, a significare un allineamento ancora solo parziale tra il regolamento sull'IA e le discipline di protezione dei dati. In questa prospettiva merita anche segnalare l'attività di redazione, in linea con gli obiettivi fissati nell'*Helsinki Statement on enhanced clarity, support and engagement*, del 2 luglio 2025 (www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf), di linee guida congiunte, in corso di predisposizione, tra l'EDPB e la Commissione per le aree di sovrapposizione/interazione tra AI Act e discipline di protezione dei dati.

47. In realtà, la tematica della *governance* si riferisce a un insieme ben più ampio di soggetti istituzionali.

48. Approccio (cui fa cenno anche la Convenzione quadro, in particolare all'art. 1, comma 2) che si risolve nell'introduzione di obblighi di diversa intensità a seconda del rischio temuto che, con un approccio *top-down*, i vari sistemi di IA, alla luce della finalità perseguita, introducono rispetto ai valori che si intendono presidiare e in ragione del quale si articolano misure diversificate di garanzia: così, per i sistemi di IA che (prospetticamente) presentano un rischio di più elevato (art. 6 del regolamento) quelle individuate agli artt. 8 ss. AI Act; o, altrimenti, misure volte a rendere riconoscibile ai singoli l'interazione con sistemi di IA considerati a rischio più limitato (art. 50 del regolamento). Secondo il medesimo approccio, ritenuto inaccettabile il rischio che talune pratiche relative all'utilizzo dei sistemi di IA comporterebbero, si sono invece introdotti più radicali divieti (art. 5 del regolamento). Per sfuggire all'inevitabile rigidità del sistema così prefigurato – che richiede un meccanismo di adeguamento continuo alle pratiche sociali connesse ai (mutevoli) impieghi di tecnologie in rapido movimento –, l'AI Act prevede tecniche di "aggiustamento" nella classificazione dei sistemi mediante atti delegati rimessi alla Commissione al fine di modificare i contenuti dell'allegato III, aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio (art. 7 AI Act). Si tratta comunque di soluzioni che, al di là delle riserve sollevate in relazione a talune scelte effettuate dal legislatore, già nella metodologia prescelta sono state ritenute non pienamente soddisfacenti: sia perché potrebbero essere sfuggite alla ricognizione tipologie di sistemi di IA che comportano esse pure rischi significativi, sia in ragione della necessità dell'intervento del legislatore, ogni qual volta emergessero applicazioni gravemente lesive di diritti individuali o di interessi di natura generale tali da richiedere l'introduzione di una nuova pratica vietata: in tal senso si è espresso l'EDPB-EDPS nella *Joint Opinion* n. 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*)», 18 giugno 2021, pt. 19. E un'esemplificazione al riguardo si sta presentando, nell'ambito dell'*Omnibus* digitale sull'IA, con l'iniziativa del Consiglio, condivisa dal Parlamento europeo, volta ad aggiungere alle fattispecie vietate dall'art. 5 dell'AI Act i sistemi di IA che alterano, manipolano o generano «artificialmente immagini o video realistici in modo da rappresentare attività sessualmente esplicite o parti intime di una persona fisica identificabile senza il suo consenso».

provider e *deployer*), pongano in essere, unitamente all'adozione di misure di cybersicurezza che tengano conto dello stato dell'arte (art. 15 AI Act), un adeguato sistema di gestione dei rischi (art. 9 AI Act) e un'appropriata *governance* dei dati utilizzati (art. 10 AI Act), al fine di assicurare l'accuratezza dei sistemi di IA e la qualità degli *output* dagli stessi prodotti, minimizzando così distorsioni e risultati discriminatori.

In questo modo, alla luce delle peculiarità delle tecnologie in parola – le cui applicazioni sociali, nella misura in cui sono venute emergendo, non si erano palesate (quantomeno nella misura in cui ora se ne prospetta l'impiego) o non avevano formato oggetto di sufficiente approfondimento (nella prospettiva regolatoria) durante la predisposizione del RGPD –, l'AI Act, da un lato, introduce alcuni divieti[49] e integra le garanzie per gli ambiti non presi in considerazione dalle discipline di protezione dei dati[50], non di rado ispirandosi ai principi da queste elaborati, ma variamente rimodellandoli[51], come nel seguito della trattazione si proverà a tratteggiare[52]. In altri casi[53], invece, l'AI Act è intervenuto per correggere alcune incongruità derivanti dall'applicazione della disciplina di protezione dei dati da più parti segnalate[54] ancorché, non di rado, sia possibile identificare situazioni di *win-win*, nelle quali gli adempimenti da assolvere in base a una delle due normative possono essere d'utilità per dare attuazione agli obblighi previsti nell'altra[55].

A quest'ultimo proposito, ad esempio, l'AI Act procede a "correggere il tiro" del divieto di trattamento delle categorie particolari di dati, misura (risalente alla legge francese cd. "*Informatique et Libertés*" del 1978[56]) volta a proteggere gli interessati per lo più da rischi di discriminazioni e possibili lesioni della dignità individuale[57], via via filtrata, non senza rilievi critici[58], fino all'art. 9 RGPD (e non diversamente all'art. 10 LED)[59]. All'interno di un'articolata cornice di garanzie prevista dall'art. 10, par. 5, AI Act, e in conformità con le previsioni contenute, per quanto interessa, nell'art. 9, par. 2, lett. *g*, RGPD e nell'art. 10, par. 1, lett. *a*, LED[60], la nuova cornice normativa ammette infatti l'impiego di tali tipologie di dati per rilevare e correggere le distorsioni che possono nascere da un loro utilizzo improprio nel contesto di sistemi di IA ad alto rischio (e quindi proprio per prevenire quelle discriminazioni che il divieto di trattamento nelle discipline di protezione dei dati mirava a

49. Si tratta delle fattispecie enumerate nell'art. 5 AI Act, che risolvono sul nascere la questione della liceità di taluni sistemi di IA, la cui immissione sul mercato e successivo utilizzo potrebbeto essere accordati in altre giurisdizioni e, in pari tempo, costituiscono un indice inequivoco dell'illiceità dei trattamenti che mediante gli stessi verrebbe effettuato: l'esempio classico al riguardo è il sistema di credito sociale cinese (*cfr.* J. Chin e L. Lin, *Stato di sorveglianza: la via cinese verso una nuova era del controllo sociale*, Bollati Boringhieri, Torino, 2022, *passim*).

50. Vds., *infra*, par. 4.

51. *Ivi.*

52. La ricognizione che segue non ha pretesa di esaustività e mira, nell'economia del presente contributo, a fornire un primo "fermo immagine" dell'*interplay* tra gli strumenti presi in considerazione, peraltro suscettibile di subire a breve modifiche alla luce dell'*Omnibus* digitale sull'IA. Essa, in particolare, non consente di definire con la necessaria puntualità tutte le ricadute applicative riferite alle numerose aree di sovrapposizione tra AI Act e discipline di protezione dei dati (peraltro non sempre esplicitate dalla disciplina) né mira, considerate le finalità del contributo, a un'analisi di dettaglio, attività necessaria per tracciare l'estensione degli obblighi (e dei diritti) che fanno capo ai soggetti interessati dallo sviluppo e impiego dei sistemi di IA. Per un approccio simile, in sede di primo esame della disciplina nazionale *in fieri*, vds. anche M. Cappai, *Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*, in *Federalismi*, n. 30/2024, pp. 186, 189 ss.

53. *Cfr. infra*, par. 4.

54. Ma il processo è tuttora in corso, come dimostra l'*Omnibus* digitale sull'IA.

55. *Cfr. infra*, par. 4.

56. *Cfr.* art. 31 *loi* n° 78-17 del 6 gennaio 1978, «relative à l'informatique, aux fichiers et aux libertés».

57. *Cfr.* R. Lattanzi, *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Europa dir. priv.*, 1998, p. 713.

58. *Cfr.* S. Simitis, *«Sensitive Daten»: zur Geschichte und Wirkung einer Fiktion*, in *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*, Stämpfli, Berna, 1990, p. 469.

59. Come è noto, il divieto di trattamento di categorie particolari di dati personali, avente natura generale, conosce eccezioni (menzionate nelle medesime disposizioni), ma esse non comprendono (allo stato) i trattamenti di dati personali suscettibili di essere effettuati all'interno del *lifecycle* dei sistemi di IA, segnatamente quelli in fase di sviluppo dei sistemi e dei modelli.

60. Le disposizioni richiamate fanno riferimento a trattamenti di categorie particolari di dati personali che possono essere effettuati in quanto necessari per motivi di interesse pubblico, rilevante sulla base del diritto nazionale o dell'Unione – qui la previsione contenuta nell'AI Act –, che «deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate per tutelare i diritti fondamentali e gli interessi dell'interessato», caratteristiche non a caso possedute dal richiamato art. 10, par. 5, AI Act.

contrastare)[61]: come si è detto, proprio in questo caso emerge l'obiettivo comune (prevenzione di fenomeni discriminatori e lesivi dell'identità individuale), ma le misure sono diversamente declinate per tenere conto della peculiarità dei sistemi di IA.

Ciò posto, va però osservato che l'art. 10, par. 5, AI Act ha una portata limitata, essendo riferito ai soli sistemi di IA ad alto rischio; l'esperienza ha invece evidenziato già l'urgenza di "correre ai ripari" anche per sistemi non classificati ad alto rischio che pure hanno manifestato distorsioni (anche gravi) nel proprio funzionamento – si pensi ad alcuni *chatbot* che si avvalgono di *large language models* (LLMs) –, rendendo necessari, anche rispetto ad essi (e con le medesime garanzie previste per quelli ad alto rischio), interventi volti a riconoscere e correggere i *bias* che li possono interessare: in questa prospettiva va collocata una delle proposte veicolata con l'*Omnibus* digitale sull'IA[62].

In altri ambiti, invece, l'intervento dell'AI Act, su impulso dell'innovazione tecnologica e di esigenze operative, si è caratterizzato come "additivo" rispetto alle discipline di protezione dei dati personali – sia il RGPD che la LED –, incidendo, per il tramite del *medium* costituito dai sistemi di IA, sul regime giuridico previsto per il trattamento dei dati biometrici[63]. Ciò si è verificato, ad esempio, all'art. 5, parr. 2-7, AI Act ove viene modellato *ex novo*, in chiave unitaria a livello europeo (e assicurando livelli di garanzia non superabili "al ribasso" dai legislatori nazionali), l'utilizzo per finalità di contrasto di sistemi di identificazione biometrica remota "in tempo reale" mediante il trattamento di dati biometrici in spazi pubblici (artt. 3, n. 42, e 5, parr. 2-7, AI Act), come pure l'utilizzo di sistemi di identificazione biometrica remota *a posteriori* (artt. 3, n. 43, e 26, par. 10, AI Act), il ricorso ai quali rimane comunque rimesso alla scelta effettuata dal legislatore nazionale[64] – scelta che, però, una volta effettuata, deve rispettare le condizioni (e il quadro di garanzie) dettate dall'AI Act[65].

Al di fuori dell'utilizzo di tali sistemi per finalità di contrasto, gli stessi vengono fatti rientrare tra i sistemi ad alto rischio (*cfr.* allegato III, n. 1)[66].

Ma le innovazioni introdotte dall'AI Act non si sono limitate a questa fattispecie. Con un disallineamento della definizione riferita ai dati biometrici contenuta nel suo art. 2, n. 34 rispetto a quella presente nell'art. 4, n. 14 del RGPD[67], l'AI Act fa filtrare nell'ordinamento, in parte vietandoli e in parte ascrivendoli tra i sistemi ad alto rischio, applicazioni ulteriori e particolarmente sensibili, che potranno comportare il trattamento di caratteristiche biometriche, al di là della sola finalità di identificazione prevista dal RGPD: si tratta dei sistemi di riconoscimento delle emozioni (definiti all'art. 3, n. 39, AI Act)[68] e dei sistemi di categorizzazione biometrica (definiti all'art. 3, n. 40, AI Act).

Non sono poi trascurabili le fattispecie in cui un medesimo principio generale, pur trovando applicazione in entrambe le discipline, è declinato in modo differente in ciascuna di esse: si pensi, anzitutto, al

61. Si rinvia, per una più ampia trattazione, a I. Žliobaitė e B. Custers, *Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models*, in *Artif. Intell. L.*, vol. 24, n. 2/2016, pp. 183, 197 ss.; M. van Bekkum e F. Zuiderveen Borgesius, *Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?*, in *Computer Law & Security Review*, vol. 48, aprile 2023, 105770.

62. È quanto prevede la proposta relativa all'*Omnibus* digitale sull'IA che mira a novellare l'AI Act con l'introduzione, al suo interno, dell'art. 4-*bis*, dedicato al trattamento di categorie particolari di dati personali a fini di rilevamento e mitigazione delle distorsioni per tutti i sistemi di IA (non più circoscrivendo questa possibilità ai soli sistemi ad alto rischio: di qui la nuova collocazione sistematica della disposizione, con la contestuale eliminazione dell'art. 10, par. 5, AI Act). La proposta è stata accolta con favore dal Consiglio, che l'ha trattata «con la massima priorità», definendo la propria posizione il 13 marzo 2026 con l'adozione di diverse proposte di emendamento, che saranno discusse nell'ambito del trilogo avviato con le altre istituzioni (www.consilium.europa.eu/it/press/press-releases/2026/03/13/council-agrees-position-to-streamline-rules-on-artificial-intelligence/). Anche il Parlamento europeo ha dato priorità all'esame di questo *dossier* (la cui adozione è indispensabile per differire l'applicazione della disciplina per i sistemi ad alto rischio, altrimenti prevista per il 2 agosto 2026) e ha adottato, in prima lettura, le proprie proposte di emendamento il 26 marzo 2026 [P10_TA(2026)0098, «*Semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale*» (*Omnibus* digitale sull'IA), P10TA(2026)0098].

63. Si tratta di ambito rispetto al quale l'EDPB-EDPS ha sollevato critiche nella *Joint Opinion* n. 5/2021, pt. 28 e 30 ss.

64. Sulla scorta delle disposizioni contenute negli artt. 5, par. 5, AI Act nonché 8 e 10, par. 1, lett. *a*, LED.

65. Ed è, in particolare, in ragione dell'introduzione della disciplina relativa ai sistemi di IA concernenti caratteristiche biometriche che l'AI Act annovera, tra le sue basi giuridiche, non solo l'art. 116 TFUE, ma anche l'art. 14 TFUE (*cfr.* *considerando* nn. 3 e 38).

66. Circostanza che, val solo la pena evidenziare, non implica per sé sola che i trattamenti effettuati mediante tali sistemi possano essere considerati leciti (anzitutto in base alla disciplina di protezione dei dati personali), trattandosi di circostanza che va, invece, valutata di volta in volta: vds. anche *considerando* n. 63 AI Act.

67. … e nonostante quanto contenuto nel *considerando* n. 14 AI Act.

68. Pur estranei al RGPD (e alla disciplina nazionale di protezione dei dati), hanno già formato oggetto di valutazione in talune occasioni da parte delle autorità di protezione dei dati: con riguardo al Garante, vds., ad esempio, il provv. 13 aprile 2023, n. 122, in *gpdp.it*, doc. *web* n. 9896412 (concernente un caso di *facial detection*, volto altresì a identificare lo stato d'animo dei visitatori di un museo mentre osservano le opere d'arte); vds., pure, provv. 11 gennaio 2024, n. 5, doc. *web* n. 9977020.

principio di trasparenza, che nel RGPD trova la sua principale applicazione nell'informativa da rendere agli interessati circa le caratteristiche del trattamento che li riguarda (in base agli artt. 13, 14 e 5, par. 1, lett. *a*, RGPD) ovvero in occasione dell'esercizio del diritto di accesso (art. 15 RGPD), mentre nell'AI Act assolve prioritariamente una funzione di avviso degli interessati (piuttosto che propriamente informativa) e mira, in prima approssimazione, a rendere edotti della sua esistenza i soggetti sui quali si possono riverberare gli effetti del funzionamento di un sistema di IA[69]. In questa prospettiva, l'art. 50, par. 1, AI Act pone in capo ai fornitori di determinati sistemi di IA l'obbligo, in linea di principio, di informare (*i.e.*, di avvisare) le persone fisiche del fatto di stare interagendo con un sistema di IA; come pure, rispetto ai sistemi di IA per finalità generali che generano contenuti audio, immagine, video o testuali sintetici, è richiesta l'adozione di misure volte ad assicurare che gli *output* del sistema di IA siano marcati in un formato leggibile meccanicamente e siano rilevabili come generati o manipolati artificialmente (art. 50, par. 2, AI Act). Non diversamente, i *deployers* di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica sono tenuti a informare le persone fisiche che vi sono esposte in merito al suo funzionamento, oltre a dover, più in generale, trattare i dati personali, a seconda dei casi, in conformità al RGPD o alla LED, secondo quanto previsto dall'art. 50, par. 3, AI Act[70]; e ancora, i *deployer* di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «*deep fake*» devono rendere noto che il contenuto è stato generato o manipolato artificialmente. Non diversamente, ciò è previsto anche per i *deployer* di un sistema di IA che genera o manipola testi oggetto di pubblicazione allo scopo di informare il pubblico su questioni di interesse pubblico (art. 50, par. 4, AI Act). In punto di trasparenza, meritano anche menzione ulteriori fattispecie introdotte dall'AI Act che, oltre a mutuare un comune principio di fondo, pure possono avere riflessi sulle previsioni contenute nelle discipline di protezione dei dati (e sull'attivazione dei rispetti rimedi): da un lato, l'obbligo per i *deployer* dei sistemi di IA ad alto rischio di cui all'all. III, che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche, di informare queste ultime che sono soggette all'uso del sistema di IA ad alto rischio (art. 26, par. 11, AI Act); dall'altro, il diritto, previsto dall'art. 86 AI Act, alla spiegazione dei singoli processi che conducono a una decisione da parte del *deployer* sulla base dell'*output* di un sistema di IA ad alto rischio elencato nell'all. III dell'AI Act, che riprende l'idea di fondo contenuta negli artt. 13, par. 2, lett. *f*, e 14, par. 2, lett. *g*, RGPD in ordine all'esistenza di processi decisionali automatizzati (non limitati a quelli connessi all'uso di sistemi di IA ad alto rischio) e nell'art. 15, par. 1, lett. *f*, RGPD.

Un'ulteriore fattispecie nella quale si rinviene un principio generale comune, declinato però (ancora una volta) in termini parzialmente diversi, riguarda poi il diritto ad assicurare un intervento umano in caso di decisioni fondate su un trattamento automatizzato (art. 22 RGPD), anch'esso presente sin dalle discipline di protezione dei dati delle origini[71], e in termini prossimi, contenuto anche nell'art. 14 AI Act ma, si noti, limitatamente ai sistemi di IA ad alto rischio, e quindi, da questo punto di vista, con un ambito di applicazione maggiormente ridotto rispetto alla previsione contenuta nell'art. 22, par. 3, RGPD[72]. Al di là del livello di prossimità del principio generale

69. In alcune delle fattispecie ricordate nel testo, all'avviso all'interessato può far anche seguito l'esercizio dei diritti in base al RGPD (*cfr.* art. 50, par. 3, AI Act); tale considerazione può essere estesa anche all'importante obbligo di avviso previsto, a vantaggio dei lavoratori e dei rispettivi rappresentanti, in base all'art. 26, par. 7, AI Act, in forza del quale, «prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i *deployer* che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti». Il *considerando* n. 27 dell'AI Act chiarisce le varie accezioni accolte per riempire di contenuto il termine «trasparenza», che ricomprende una pluralità di dimensioni (ciascuna delle quali può essere servente nei confronti delle altre): la "tracciabilità" delle operazioni effettuate tramite un sistema di IA; la "spiegabilità" del modo in cui il sistema opera (per contrastare l'effetto *black box*, sul quale vds. l'ormai classico studio di F. Pasquale, *The black box society: the secret algorithms that control money and information*, Harvard University Press, Cambridge (MA), 2015, *passim*, e, sulle possibili contromisure, vds. S. Wachter - B. Mittelstadt - C. Russell, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR*, in *Harv. J. Law Technol.*, vol. 31, 2018); le misure da adottare per rendere «gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA»; infine, in una dimensione più prossima agli obblighi di informazione contrattuali, il flusso informativo (comprese le istruzioni di funzionamento del sistema) tra *provider* e *deployer* (in ultima analisi, funzionale anche a rendere comprensibile ai soggetti interessati dal loro uso il funzionamento del sistema).

70. Disposizione che, come già l'art. 2, par. 7, AI Act, viene a costituire un ulteriore punto di emersione della necessaria complementarità nell'applicazione delle discipline di protezione dei dati con l'AI Act.

71. *Cfr.* art. 2 loi n° 78-17 del 6 gennaio 1978, che ha poi influenzato la redazione dell'art. 15 della direttiva 95/46/CE.

72. Previsione che, a sua volta, può trovare applicazione solo nei casi previsti dall'art. 22, par. 2, lett. *a* e *c*, RGPD.

di riferimento (volto ad assicurare la possibilità di un intervento umano rispetto a effetti che possano avere impatti significativi sugli individui), va però osservato che l'art. 14 AI Act mira prioritariamente ad assicurare la sorveglianza umana sul complessivo funzionamento del sistema di IA ad alto rischio (mediante misure integrate nello stesso da parte del fornitore o che possono richiedere l'intervento del *deployer* tramite persone fisiche che abbiano le caratteristiche per poter effettivamente comprendere e monitorare il funzionamento del sistema e interpretarne gli *output*, sino al punto di intervenire sul suo funzionamento, interrompendolo ovvero disattendendone gli *output*)[73], mentre l'art. 22, par. 3, RGPD ha il proprio *focus* (più circoscritto rispetto alle varie misure di sorveglianza umana contenute nell'art. 14 AI Act) nel possibile riesame della decisione individuale basata unicamente[74] sul trattamento automatizzato (indipendentemente, quindi, dal fatto che sia utilizzato un sistema di IA ad alto rischio).

In altre circostanze, gli adempimenti da assolvere in base a una delle due normative possono poi risultare utili per dare attuazione agli obblighi previsti nell'altra: oltre alla fattispecie appena ricordata – nella quale la corretta attuazione delle misure previste dall'art. 14 AI Act possono agevolare (se non addirittura rendere possibile) l'adempimento dell'obbligo previsto dall'art. 22, par. 3, RGPD –, altri sono i casi che possono essere menzionati e che rendono palese l'utilità di sinergie tra le misure introdotte dall'AI Act e delle discipline di protezione dei dati. Si pensi, ad esempio, all'art. 26, par. 9, AI Act, il quale dispone che le informazioni riferite al funzionamento del sistema di IA fornite dal *provider* al *deployer* possono essere utilizzate ai fini della valutazione d'impatto sulla protezione dei dati (DPIA prevista dall'art. 35 RGPD o dall'art. 27 LED); e quest'ultima, a sua volta, può risultare utile in vista della valutazione d'impatto sui diritti fondamentali (FRIA) prevista, per talune fattispecie[75], dall'art. 27 AI Act. Ma le stesse informazioni, oltre a quelle contenute nelle istruzioni per l'uso fornite, in base all'articolo 13 AI Act, dal *provider* al *deployer*, possono da quest'ultimo essere utilizzate per l'eventuale predisposizione dell'informativa agli interessati ai sensi degli artt. 13 e 14 del RGPD[76] o possono contribuire a fornire elementi utili in vista del riscontro da rendere agli interessati in caso di esercizio del diritto d'accesso previsto dall'art. 15, par. 1, lett. *h*, RGPD.

A ben vedere, non mancano altri casi in cui, in termini analoghi, l'assolvimento di taluni obblighi previsti all'interno di uno dei due silos regolatori può rivelarsi funzionale anche a soddisfare (magari solo indirettamente) uno dei requisiti previsti dall'altra disciplina: si pensi alle misure da adattare per dare attuazione al principio di accuratezza e aggiornamento dei dati personali previsto dall'art. 5, par. 1, lett. *d* del RGPD, che può dispiegare i propri effetti anche per assicurare che «i *set* di dati di addestramento, convalida e prova [siano,] nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista», contribuendo così a rispettare la previsione dell'art. 10, par. 3, AI Act.

E anche la previsione contenuta nell'art. 10, par. 2, AI Act, nella parte in cui prevede, tra le pratiche di *governance* e gestione dei dati di addestramento, convalida e prova, quelle riguardanti «i processi di raccolta dei dati e l'origine dei dati, nonché la finalità originaria della raccolta nel caso di dati personali», pare orientata a consentire il rispetto della disciplina di protezione dei dati e, in particolare, del principio di finalità (artt. 5, par. 1, lett. *b*, e 6, par. 4, RGPD) nella fase di sviluppo dei sistemi di IA ad alto rischio. Principio di finalità che non viene meno in relazione ai trattamenti di dati personali nel contesto dello sviluppo dei sistemi di IA, come peraltro si desume anche *a contrario* dalla disposizione contenuta nell'art. 59 AI Act, che a questo riguardo reca un'eccezione per consentire, nell'ambito degli spazi di sperimentazione normativa per l'IA, i trattamenti di dati personali legalmente raccolti per altre finalità[77].

Val solo la pena precisare che il vantaggio reciproco che in taluni casi può derivare dall'attuazione di segmenti delle due discipline non necessariamente comporta, come non di rado viene lamentato, appesantimenti burocratici. L'AI Act, infatti, ragio-

73. *Cfr*. art. 14, par. 3, AI Act.

74. Sul significato di decisione «fondata esclusivamente su un trattamento automatizzato», vds. la sentenza della Corte di giustizia del 7 dicembre 2023, C-634/21, *Schufa*.

75. *Cfr*. art. 5, par. 2, secondo periodo, AI Act.

76. In particolare, con riguardo all'art. 13, par. 2, lett *f*, e all'art. 14, par. 2, lett. *g*, in relazione «all'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

77. ... con l'ulteriore precisazione che, in questo contesto, i dati possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando sono soddisfatte particolari condizioni, tra le quali, in primo luogo, che i sistemi di IA siano sviluppati per salvaguardare un interesse pubblico rilevante.

nevolmente dispone che, ove adempimenti anche solo in parte di identica natura siano previsti da una disciplina, essi non devono essere reiterati per dare attuazione all'altra: il caso che in proposito può venire in gioco è quello della FRIA che, ove abbia già formato oggetto di attuazione (ancorché parziale) mediante la DPIA, non deve essere duplicata da parte del *provider*, ma può essere integrata nella FRIA (art. 27, par. 4, AI Act). Alle medesime conclusioni l'AI Act addiviene anche in relazione alla previsione dell'art. 86, par. 3, in presenza di altre disposizioni del diritto dell'Unione che prevedano il diritto ad ottenere una spiegazione circa i singoli processi decisionali[78].

5. Verso una *governance* integrata? Non ancora... ma a che prezzo?

Quanto l'analisi del dato normativo lascia trasparire è l'idea della necessità – per restare fedeli alle scelte operate con l'AI Act, che si pongono in linea di continuità con il disegno della Carta dei diritti fondamentali – di una coerente e complementare applicazione delle disposizioni presenti nei due plessi normativi, attraverso l'esplorazione delle opzioni interpretative percorribili in base al diritto vigente, ove difficoltà applicative dovessero emergere[79], e l'individuazione, ove necessario, dei termini di possibili adeguamenti normativi[80]. Si tratta di un percorso talvolta faticoso[81], ma non impraticabile: un giudizio "secco" di incompatibilità tra le discipline di protezione dei dati e le applicazioni basate sulle tecniche di IA[82] non è quindi, alla luce del quadro di garanzie dettate dall'AI Act, un esito ineluttabile (per quanto possa apparire il più sbrigativo)[83]. Né, per vero, è il risultato voluto dall'AI Act. La direzione presa dal legislatore europeo è, piuttosto, come abbiamo visto, quella della complementarità e dell'integrazione tra le misure previste nell'AI Act e quelle proprie delle discipline di protezione dei dati personali.

Resta allora da capire quanto questo approccio – che riguarda le regole che devono trovare applicazione nello sviluppo e uso dei sistemi di IA – si rispecchi nella cornice istituzionale volta a presidiare il corretto utilizzo dei sistemi di IA. Senza voler qui trattare *ex professo* il disegno (articolato) di *governance* previsto dall'AI Act[84] – vale a dire l'insieme degli strumenti volti ad assicurare un controllo efficace dell'insieme di misure che con l'AI Act si sono volute introdurre per creare le premesse di una IA (che possa quantomeno aspirare ad essere) *trustworthy* e antropocentrica –, basti dire che, anche da questo punto di vista, l'AI Act contiene elementi volti a mettere in comunicazione i distinti silos normativi grazie a puntuali disposizioni in materia di obblighi di consultazione[85] e di comu-

78. Fattispecie che non è limitata alle ipotesi analoghe presenti nelle discipline di protezione dei dati: si pensi, ad esempio, alla fattispecie prevista dall'art. 11 della direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, in caso di decisione assunta mediante un sistema di IA (da considerare ad alto rischio, in quanto riconducibile tra quelli previsti dall'all. III, n. 4, lett. *b*, AI Act). E non diversamente deve argomentarsi, in materia di credito al consumo, in relazione al diritto di ottenere una spiegazione significativa e comprensibile della valutazione effettuata e del funzionamento del trattamento automatizzato applicato, compresi le principali variabili, la logica e i rischi inerenti, previsto dall'art. 18, par. 8, lett. *a*, direttiva (UE) 2023/2225 del Parlamento europeo e del Consiglio, del 18 ottobre 2023, relativa ai contratti di credito ai consumatori, e che abroga la direttiva 2008/48/CE, nel caso sia effettuato mediante un sistema di IA (da considerare ad alto rischio, in quanto riconducibile tra quelli previsti dall'all. III, n. 5, lett. *b*, AI Act).

79. In questo senso, quanto al possibile ricorso al legittimo interesse quale base giuridica per i trattamenti di dati personali, vds. EDPB *Opinion* n. 28/2024 «*on certain data protection aspects related to the processing of personal data in the context of AI models*», 17 dicembre 2024.

80. In questo senso, vds. *supra*, par. 4.

81. E una «difficile convivenza» era stata già prefigurata dal Garante per la protezione dei dati personali nell'ambito dell'indagine congiunta realizzata con AGCM e AGCom nella *Indagine conoscitiva sui Big Data* (www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf), i cui esiti sono stati resi pubblici il 10 febbraio 2020, pp. 48, 52 ss.

82. *Cfr*. T.Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, vol. 47 *Seton Hall L. Rev*., vol. 47, n. 4/2017, pp. 995, 1004 ss.

83. Ma, bisognerebbe allora chiedersi, a vantaggio (o a danno) di chi deporrebbero scelte volte a spostare i punti di equilibrio tra i valori in gioco? È davvero nel complessivo sistema di tutela dei diritti che ha caratterizzato (con tutti i suoi limiti) l'azione dell'Unione europea, non solo nel settore della protezione dei dati (vds., in merito, lo studio classico di A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020, *passim*) e ora dell'IA, che si radicano le ragioni della dichiarata arretratezza tecnologica rispetto ai due principali attori sulla scena globale, (al momento) Stati Uniti e Cina?

84. Per una più ampia trattazione si rinvia a R. Lattanzi, *AI Act e autorità di protezione dei dati personali*, *op. cit*., part. pp. 382 ss. Vds. pure il contributo, dal titolo significativo, di S. Villani, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE*, Speciale n. 2/2024 (www.aisdue.eu/wp-content/uploads/2024/06/Post-Susanna-Villani.pdf).

85. *Cfr*. art. 79 AI Act.

nicazione[86] tra le autorità di vigilanza del mercato[87] e le autorità di tutela dei diritti fondamentali di cui all'art. 77 AI Act[88], affinché ciascuna di esse sia messa in condizione di assolvere al meglio la propria missione istituzionale.

Ed anzi, tenendo almeno in parte conto delle indicazioni formulate dall'EDPB[89], l'AI Act fa, all'art. 74, par. 8, un passo avanti nella direzione (che va al di là della mera cooperazione tra autorità) dell'ibridazione dei modelli, prevedendo per taluni sistemi di IA ad alto rischio che le autorità di protezione dei dati personali siano altresì chiamate ad operare, e in questa prospettiva designate dagli Stati membri, quali autorità di vigilanza del mercato. La richiamata disposizione, all'evidente scopo di innalzare negli ambiti considerati il livello di garanzia, prevede infatti che «per i sistemi di IA ad alto rischio elencati nell'allegato III del (...) regolamento, punto 1[90], nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III [dell'AI Act], punti 6[91], 7[92] e 8[93], gli Stati membri [designino] come autorità di vigilanza del mercato ai fini [dell'AI Act] le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680».

Come è noto, a questa disposizione il legislatore italiano non ha dato attuazione nei termini previsti dall'AI Act, atteso che la l. 23 settembre 2025, n. 132 (in particolare, all'art. 20) ha attribuito la qualità di autorità di vigilanza del mercato negli ambiti testé ricordati all'Agenzia per la cybersicurezza nazionale (ACN) – che non soddisfa i requisiti di indipendenza richiesti dall'art. 75, par. 8, AI Act, in quanto agenzia governativa e non autorità indipendente – e non al Garante per la protezione dei dati personali[94].

E le conseguenze di questa scelta non si arrestano alla sola possibile attivazione di una procedura di infrazione nei confronti dell'Italia da parte della Commissione europea, ma introducono un elemento di instabilità nel nostro ordinamento: da un lato, infatti, l'ACN sarebbe tenuta a disapplicare la disciplina nazionale che si pone in contrasto (in questo caso, palese) con il diritto dell'Unione. Dall'altro, indipendentemente dalle determinazioni dell'ACN, ove quest'ultima dovesse comunque assumere determinazioni negli ambiti individuati dall'art. 74, par. 8, AI

86. *Cfr*. artt. 77, par. 1, e 73, par. 7, AI Act, in ordine all'obbligo di notifica, da parte dell'autorità di vigilanza del mercato, di casi di «*serious incident*».

87. La cui definizione è resa all'art. 3, n. 26, AI Act.

88. Esse comprendono gli organismi per la parità e le autorità per la protezione dei dati: *cfr*. *considerando* n. 157.

89. In merito, vds. *Statement* n. 3/2024 «on data protection authorities' role in the Artificial Intelligence Act framework», 16 luglio 2024 (www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_en), nel quale si illustrano le ragioni per designare le autorità di protezione dei dati quali autorità di vigilanza del mercato con riguardo alle fattispecie individuate nell'all. III (con l'eccezione del caso previsto al suo n. 2) e si ribadisce l'obbligo, per gli Stati membri, di procedere quantomeno alla designazione delle stesse per i casi indicati nell'art. 74, par. 8, AI Act.

90. I sistemi biometrici, vale a dire (in prima approssimazione) i sistemi di identificazione biometrica remota, i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti, basati sulla deduzione di tali attributi o caratteristiche, e i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni.

91. Alcuni sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto.

92. Alcuni sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, in relazione alle materie della migrazione, dell'asilo e del controllo delle frontiere.

93. I sistemi di IA destinati a essere utilizzati nell'amministrazione della giustizia e nell'ambito dei processi democratici, nonché i sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un *referendum* o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai *referendum*.

94. Più diffusamente, su questi profili, mi sono soffermato in *AI Act e autorità di protezione dei dati personali*, *op. cit*., part. pp. 382 ss. (cui si rinvia). In questo senso si esprimono anche M. Rabitti e F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, in *Iid.* (a cura di), *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, Roma Tre-Press, 2025, pp. 13, 22. Pur ripercorrendo le posizioni dell'EDPB nei documenti in precedenza indicati e dallo stesso Garante, non prende però posizione sul punto M. Cappai, *Garante per la protezione dei dati personali. Protezione dei dati personali e intelligenza artificiale: quale governance?*, in M. Rabitti e F. Bassan, *op. ult. cit*., pp. 29, 36 (e in *Federalismi*, n. 30/2024, p. 186), il quale sembra però implicitamente ammettere la conformità all'AI Act di una scelta che, per i sistemi di IA indicati dall'art. 74, par. 8, AI Act, non cada sul Garante (o comunque, dovrebbe arguirsi, su un'autorità altra, esistente o di nuova istituzione, che soddisfi però un equivalente livello di indipendenza): «La posizione assunta dall'EDPB e dal Garante *privacy* appare animata dalle migliori intenzioni e denota, indubbiamente, un certo pragmatismo. Ciò non equivale a dire, però, che una scelta legislativa di segno diverso sarebbe automaticamente contraria al regolamento IA o determinerebbe di per sé un pregiudizio alla protezione dei dati personali»: ma qui, val la pena osservare, non vengono in questione ragioni di opportunità, quanto di osservanza della (specifica) previsione contenuta nell'AI Act.

Act, queste potrebbero essere sottoposte a sindacato giurisdizionale e caducate[95].

Al netto di questi profili, la disciplina nazionale non ha ancora introdotto forme strutturate di cooperazione che diano attuazione alla previsione contenuta nell'art. 74, par. 10, AI Act – salva l'individuazione del Comitato di coordinamento previsto dall'art. 20, comma 3, l. n. 132/2025[96] –, a fronte della necessità, ormai largamente avvertita, di irrobustire la cooperazione e l'efficacia dell'*enforcement* nel settore digitale: in questa direzione si sono decisamente mossi, sulla spinta iniziale dell'esperienza britannica, con l'istituzione avvenuta nel 2020 del *Digital Regulation Cooperation Forum*, gli ordinamenti più dinamici nell'economia digitale[97], recuperando così l'idea di una *Digital Clearing House*[98]. Idea che, peraltro, anche nell'ordinamento nazionale ha iniziato ad attecchire e a trovare una forma di concretizzazione nelle modalità di funzionamento del Comitato *fintech* ("laboratorio" che vede il coinvolgimento in chiave cooperativa di una pluralità di autorità indipendenti e soggetti istituzionali)[99] e che, in chiave prospettica, comunque dovrà trovare applicazione nelle *sandbox* previste dall'AI Act, con la necessaria partecipazione, in caso di sistemi di IA che comportino il trattamento di dati personali, anche del Garante[100].

Potrebbe forse essere l'adozione dei decreti legislativi previsti dalla l. n. 132/2025 l'occasione propizia per individuare formule adeguate di interazione.

Deve infine aggiungersi che, in punto di *governance*, non è però solo il livello nazionale (almeno nel caso italiano) a suscitare le sopra ricordate riserve, ma anche quello, sovraordinato, che vede quale soggetto incaricato dell'attività di supervisione, in qualità autorità di vigilanza del mercato, il solo *AI Office* in relazione ai sistemi di IA e dei modelli di IA per finalità generali disciplinati nel capo V dell'AI Act[101], senza che quest'ultimo abbia previsto, per i profili relativi al

95. In merito, vds. Cons. Stato, sez. VI, 7 marzo 2025, n. 1406 (e ivi più risalenti precedenti), secondo cui, «fermo restando che il contrasto tra un provvedimento amministrativo nazionale e il diritto dell'Unione europea debba generare qualche forma d'invalidità dell'atto in questione, il Consiglio di Stato, almeno a far tempo dalla sentenza di questa Sezione 31 marzo 2011, n. 1983, ha affermato che l'atto amministrativo che viola il diritto dell'Unione europea è affetto da annullabilità per vizio di illegittimità sotto forma di violazione di legge e non da nullità, atteso che l'art. 21-*septies* della l. 7.8.1990, n. 241, ha codificato in numero chiuso le ipotesi di nullità del provvedimento amministrativo e tra queste ipotesi non rientra il contrasto con il diritto dell'Unione europea. Ne consegue che la nullità è configurabile nella sola ipotesi in cui il provvedimento amministrativo nazionale sia stato adottato sulla base di una norma interna attributiva del potere incompatibile con il diritto europeo e quindi disapplicabile (...)». Ripercorre adesivamente questo orientamento consolidato della giustizia amministrativa A. Cacciari, *La sorte del provvedimento in contrasto con il diritto dell'U.E. o con la Convenzione Edu*, relazione tenuta al Corso di formazione per magistrati amministrativi di prima nomina, organizzato dall'Ufficio studi e formazione della Giustizia amministrativa, 10 gennaio 2025 (www.giustizia-amministrativa.it/-/158189-151).

96. L'art. 20, comma 3, l. n. 132/2025, dispone che «Le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo. A quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima. Al suddetto Comitato partecipano, quando si trattano questioni di rispettiva competenza, rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS. (...)». La disposizione non chiarisce se e in che forma siano chiamate ad interagire con esso le autorità di tutela dei diritti fondamentali (e, tra queste, il Garante), rispetto alle quali continuerebbero quindi a valere solo gli obblighi di avviso e di consultazione indicati dall'AI Act.

97. Iniziative analoghe sono, per l'Olanda, la *Digital Regulation Cooperation Platform* (SDT); per l'Australia, il *Digital Platform Regulators Forum* (DP-REG); per il Canada, il *Canadian Digital Regulators Forum* (CDRF) e, per l'Irlanda, il *Digital Regulators Group*. Per ulteriori indicazioni, vds. anche M. Cappai, *Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146*, *op. cit.*, pp. 186, 201 ss.

98. *Cfr.* EDPS, *Opinion* n. 8/2016 «*on coherent enforcement of fundamental rights in the age of big data*»:
«The Clearing House would be a voluntary network of contact points in regulatory authorities at national and EU level who are responsible for regulation of the digital sector, which might also include authorities such as those in the telecommunications area who supervise the implementation of rules on confidentiality of communications. The two criteria for joining this network would be:
1. a shared aim of mutually enhancing their respective enforcement activities and of delivering the best outcome for individuals' rights and welfare, whether as consumers or data subjects;
2. a willingness to share information and to collaborate within the boundaries of legal competences and respecting the confidentiality of investigatory activities».

99. *Cfr.* art. 36, commi da 2-*bis* a 2-*septies*, l. 28 giugno 2019, n. 58, di conversione del dl 30 aprile 2019, n. 34, che ha introdotto anche la disciplina dei cd. "*regulatory sandbox*", nonché il decreto del Ministro dell'economia e delle finanze, recante attuazione dell'art. 36, commi 2-*bis* ss., dl 30 aprile 2019, n. 34 (conv., con modif., dalla l. 28 giugno 2019, n. 58) sulla disciplina del Comitato e della sperimentazione *fintech*.

100. *Cfr.* art. 57, par. 10, AI Act.

101. L'ufficio per l'IA, che non ha caratteristiche di indipendenza, è «la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della *governance* dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione» (art. 3, n. 47, AI Act). In base all'art. 75, par. 1, AI Act, nell'assolvimento di tali compiti l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato e di quelli previsti dal regolamento (UE) 2019/1020 e, in base all'art. 88, par. 1, AI Act, la Commissione, che ha «competenze esclusive per la vigilanza e l'esecuzione del capo V», «affida l'attuazione di tali compiti all'ufficio per l'IA».

trattamento dei dati personali, forme di raccordo con le autorità di protezione dei dati[102].

Anche a tale proposito, in ragione della clausola generale della "*sincere cooperation*", cui già la Corte di giustizia ha fatto ricorso nel caso *Meta*[103], e pur nel rispetto dell'indipendenza che deve caratterizzare l'operato di ciascuno degli attori istituzionali, è urgente individuare più precise modalità di cooperazione affinché, anche rispetto ai sistemi di IA rientranti nelle attribuzioni dell'*AI Office* (non diversamente da quelli rilevanti al livello nazionale), sia comunque pienamente salvaguardato il requisito della supervisione indipendente previsto dall'art. 8, par. 3 della Carta dei diritti fondamentali dell'Unione.

Nei limiti della riflessione che si è condotta, può allora essere utile ritornare alle parole di Giovanni Buttarelli, contenute nelle conclusioni del parere dell'EDPS n. 4/2015, finalizzato a fornire un contributo affinché «l'UE possa garantire l'integrità dei propri valori, sfruttando al contempo i vantaggi delle nuove tecnologie»: «la protezione della vita privata e dei dati costituisce parte della soluzione e non del problema. Per il momento, la tecnologia è controllata da esseri umani. (...) I principi di protezione dei dati si sono dimostrati in grado di salvaguardare le persone e la loro vita privata dai rischi di trattamenti irresponsabili. Tuttavia, le attuali tendenze possono richiedere un approccio del tutto innovativo»[104].

In questa prospettiva, un'opera di consapevole e paziente tessitura di un più articolato concerto istituzionale può contribuire a inverare il progetto di una IA autenticamente antropocentrica senza correre il rischio di andare, per l'appunto, in ordine sparso[105].

102. Si tratta di profilo critico già evidenziato nel menzionato EDPB *Statement* n. 3/2024 «*on data protection authorities' role in the Artificial Intelligence Act framework*», pt. 15.

103. CGUE (GS), 4 luglio 2023, C-252/21, *Meta*.

104. Garante europeo della protezione dei dati, parere n. 4/2015, «*Verso una nuova etica digitale. Dati, dignità e tecnologia*», 11 settembre 2015, p. 17.

105. Per mutuare il titolo di Villani: *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, *op. cit.*