ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

FOCUS LAVORO, PERSONA, TECNOLOGIA
18 DICEMBRE 2024

Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?

di Marco Cappai
Assegnista di ricerca in Diritto amministrativo
Università degli Studi di Roma Tre

Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*

di Marco Cappai
Assegnista di ricerca in Diritto amministrativo
Università degli Studi di Roma Tre

Abstract [It]: Descritto il rapporto tra intelligenza artificiale (IA) e privacy, ed esaminata la *governance* europea dell'IA, il contributo tenta di individuare, anche alla luce della più recente attività di *enforcement* del Garante per la protezione dei dati personali (GPDP), l'assetto istituzionale ottimale sul piano del diritto interno. Prendendo le mosse dal modello tratteggiato nel d.d.l. n. 1146, e tenuto conto di quanto sta avvenendo in altri sistemi giuridici, si propone una formula allocativa dei pubblici poteri in grado di preservare il ruolo di custode del diritto alla protezione dei dati personali affidato al GPDP, senza per questo menomare gli obiettivi, indubbiamente anche di politica economica, che sembrano emergere dal cantiere normativo in corso.

Title: Artificial intelligence and personal data protection in the d.d.D. n. 1146: which national governance?
Abstract [En]: After having described the relationship between artificial intelligence (AI) and privacy, and following an overview on the AI Act, the contribution seeks to identify, also in light of the most recent enforcement activity of the Garante per la protezione dei dati personali (GPDP), the optimal institutional design in domestic law. Moving from the model envisaged in Bill No. 1146, and taking into account what is happening in other legal systems, an allocative formula of public powers is proposed that is capable of preserving the GPDP's role as guardian of the right to personal data protection, without undermining the objectives, undoubtedly also of economic policy, that seem to be emerging from the ongoing legislative process.

Parole chiave: IA; privacy; assetto istituzionale
Keywords: AI; privacy; institutional design

1. Il rapporto tra intelligenza artificiale e *privacy*

Il fenomeno dell'intelligenza artificiale ("IA"), non è mistero, rappresenta un'assoluta priorità nell'agenda legislativa globale[1].

* Articolo sottoposto a referaggio. L'articolo costituisce uno sviluppo del Capitolo dal titolo "*Protezione dei dati personali e intelligenza artificiale: quale* governance*?*" per la ricerca Consumerism 2024, Diciassettesimo rapporto annuale, *Intelligenza Artificiale e protezione dei consumatori: il ruolo delle Authorities e delle Agenzie nazionali*, curata da F. BASSAN e M. RABITTI e presentata il 27 novembre 2024, in partic. 25 ss.

[1] D. CLEMENTI, *Generare e non creare? Spunti per una comparazione sulla regolazione dell'intelligenza artificiale generativa tra Stati Uniti, Repubblica Popolare Cinese e Unione Europea*, in *Rivista di diritti comparati*, n. 2/2024, 371 ss.; B. MARCHETTI - L. PARONA, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *Diritto pubblico comparato ed europeo Online*, n. 1/2022, n. 237 ss.

Solo nel mese di novembre si sono conclusi i negoziati affidati al Comitato sull'intelligenza artificiale (CAI) del Consiglio d'Europa, con l'adozione, a Vilnius, di un'ambiziosa Convenzione quadro su IA, diritti umani e Stato di diritto[2]; inoltre, il Select Committee on Adopting Artificial Intelligence (AI), nominato lo scorso marzo dal Senate australiano, ha prodotto un articolato report in cui ha formulato 13 raccomandazioni[3].

Ancora una volta, tuttavia, il primato regolatorio è dell'Unione europea, che a giugno 2024 ha approvato il Regolamento IA, per giudizio unanime la prima disciplina organica in materia[4].

Il Regolamento si radica sulla competenza di ravvicinamento delle disposizioni nazionali per l'instaurazione ed il funzionamento del mercato interno[5], nonché sulla competenza in materia di protezione dei dati personali[6]. L'opzione per la forma tipica del regolamento è conforme ai princìpi di sussidiarietà e proporzionalità, in quanto la frammentazione del quadro giuridico di riferimento determinerebbe, in questa peculiare materia: i) un sistema di tutele a macchia di leopardo; ii) un disincentivo all'innovazione[7].

Proprio per questa ragione il Regolamento ha adottato un approccio di uniformazione di natura orizzontale. Pone dei requisiti minimi di natura scalare, secondo l'approccio *risk based* oramai consolidato nella legislazione europea[8]. Sfuggono alla piramide regolatoria i sistemi di IA con rischi minimi o nulli, che non sono regolati, mentre ne costituiscono la base i sistemi di IA con rischi limitati, sottoposti a soli obblighi di trasparenza; nel centro, troviamo i sistemi di IA con rischi elevati, soggetti a più pervasivi

[2] Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, siglata a Vilnius il 5 novembre 2024 e sottoscritta, per l'Unione europea, dalla Commissione, nonché la metodologia "for the risk and impact assessment of artificial intelligence systems from the point of view of Human rights, Democracy and the Rule of law" (HUDERIA methodology), approvata a Strasburgo il 26-28 novembre 2024 nella 12esima seduta plenaria del Committee on Artificial Intelligence (CAI). In argomento, v. A. MANTELERO - F. FANUCCI, *The International Debate on AI Regulation and Human Rights in the Prism of the Council of Europe's CAHAI: Great Ambitions*, in P. Czech - L. Heschl - K. Lukas - M. Nowak - G. Oberleitner (a cura di), *European Yearbook on Human Rights 2022*, Intersentia, 2022, 225 ss.; L. COTINO HUESO, *The Council of Europe's Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, n. 3/2024, 53 ss.

[3] Final Report, 26 novembre 2024.

[4] Il Regolamento (UE) 2024/1689 del 13 giugno 2024 "*che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)*". Per una prima lettura della proposta di regolamento, L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023, in partic. Cap. V; per un commentario al testo definitivo, C. NECATI PEHLIVAN - N. FORGÓ, - P. VALCKE (a cura di), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2024.

[5] Art. 114 TFUE.

[6] Artt. 16 TFUE e 8 CDFUE.

[7] Conss. nn. 8 e 9 del Regolamento IA.

[8] G. DE GREGORIO - P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, n. 59(2)/2022, 473 ss.; M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, in *Journal of European Journal of Risk Regulation*, 2024, 1 ss. Per una riflessione più generale, A. BARONE, *Il diritto del rischio*, Milano, 2006.

poteri di controllo preventivo e vigilanza *ex post*; al vertice, infine, vi è l'utilizzo dei sistemi di IA che pongono rischi inaccettabili e, come tali, sono sempre vietati.

I requisiti e divieti posti dal Regolamento sono uniformi in tutto il territorio dell'Unione e ineriscono, essenzialmente, all'affidabilità (*trustworthiness*) della tecnologia. Tale anima del regolamento riflette un *product safety approach* e, non a caso, si intreccia, in larga parte, con la disciplina europea in materia di sicurezza dei prodotti.

Al contempo, la protezione dei "valori europei" rappresenta una dichiarata finalità del Regolamento, che intende coniugare il carattere dell'affidabilità con quello dell'"antropocentrismo" della tecnologia[9], al fine di assicurare che l'IA sia rispettosa dei diritti fondamentali (*rights based appraoch*)[10].

Tra questi, quello alla protezione dei dati personali assume, senza dubbio, un rilievo centrale, come del resto già riconosciuto, in sede internazionale, dall'OECD[11] e, prima ancora, dall'Independent High-Level Expert Group on Artificial Intelligence nominato dalla Commissione europea[12].

Da ultimo, anche le Autorità di protezione dei dati personali del G7 hanno evidenziato che "*many AI technologies, including generative AI, are based on the processing of personal data, which can subject natural persons to unfair stereotyping, bias and discrimination even when not directly processing their respective personal data. This, in turn, may influence larger societal processes with deep fakes and disinformation. Consequently, data protection and the need to protect the right to privacy are more critical than ever*"[13].

Coerentemente con la descritta impostazione *rights based*, il Regolamento "*non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione del diritto dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati*"[14], prevedendo espressamente che "*il diritto dell'Unione in materia di protezione dei dati personali … si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento*". Resta dunque "*impregiudicat*[o] *il regolamento (UE) 2016/679*", fatte salve le previsioni specifiche poste, in punto di trattamento dei dati personali, dal Regolamento[15].

Tra la disciplina dell'IA e la tutela della privacy possono individuarsi tre principali tipologie di rapporto:

---

[9] Cons. 1 e art. 1 del Regolamento IA.

[10] Tra i molti, T. EVAS, *The EU Artificial Intelligence Act: Advancing Innovation for Trustworthy AI*, in *AIRe*, n. 2/2024, 89 ss. In senso critico, v. M. ALMADA - A. RADU, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *German Law Journal*, n. 25(4)/2024, 646 ss., secondo i quali, almeno nella proposta di regolamento oggetto di accordo politico provvisorio a gennaio 2024, l'approccio *rights based* sarebbe recessivo rispetto a quello di *product safety*, con inevitabili ricadute, anche extraeuropee, sulla *governance* dell'IA.

[11] *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, 2024, § 1.2.a.

[12] *Ethics Guidelines for Trustworthy AI*, 8 aprile 2019.

[13] *Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI*, 11 ottobre 2024, § 6.

[14] Cons. 157 del Regolamento IA.

[15] In particolare, l'art. 2, § 7 del Regolamento IA fa esplicito riferimento agli artt. 10, § 5 e 59, su cui si tornerà *infra*.

a) Sovrapposizione/Duplicazione: in non pochi casi, il Regolamento IA e il Regolamento generale sulla protezione dei dati ("GDPR")[16] convergono su aspetti specifici, disciplinando, sotto diversi e complementari punti di vista, il medesimo fenomeno. Si pensi al diritto dell'interessato, sancito all'art. 22 GDPR, "*di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Come intuibile, decisioni automatizzate di questo genere hanno tipicamente luogo tramite sistemi di IA. Proprio per tale ragione, il Regolamento IA precisa che, in aggiunta a quanto previsto nel regolamento stesso, "*gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione*"[17]. Ancora, l'affidabilità dei sistemi di IA è garantita anche attraverso "*misure tecniche e organizzative*"[18] e "*misure volte a prevenire … gli attacchi alla riservatezza*"[19], le quali si affiancano, senza sostituirle, alle cc.dd. "*misure di sicurezza*" previste dal GDPR[20]. Per fare un ulteriore esempio, poi, così come in caso di c.d. *data breach* entrano in azione i presìdi di cui all'art. 33 GDPR, il Regolamento IA delinea un obbligo di "*condivisione di informazioni su incidenti gravi*"[21], avendo cura di precisare, nella parte definitoria, che costituisce "*incidente grave*", tra l'altro, "*la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali*"[22]. In tutti questi casi, dunque, i due plessi disciplinari si applicano in via cumulativa e parallela, rinsaldandosi a vicenda;

b) Integrazione: nel prendere atto delle descritte sovrapposizioni, in altri casi il legislatore europeo ha cercato, per esigenze di razionalizzazione e semplificazione del sistema, di tracciare un rapporto di integrazione tra le due discipline. Tale operazione coinvolge tanto l'anima del Regolamento caratterizzata da un *product safety approach*[23], tanto, per ciò che qui interessa, la componente espressiva di un *rights based approach*. Per esempio, si prevede che le valutazioni d'impatto sui diritti fondamentali (*fundamental rights impact assessment* - FRIA) per i sistemi di IA ad alto rischio[24] valgano anche, con le dovute addizioni, agli effetti della

[16] Regolamento (UE) 2016/679.
[17] Cons. 10 del Regolamento IA.
[18] Art. 15, § 4 del Regolamento IA.
[19] Art. 15, § 5 del Regolamento IA.
[20] Segnatamente, art. 32 e cons. 83 del GDPR.
[21] Art. 73 del Regolamento IA.
[22] Art. 3, n. 49, lett. *c)* del Regolamento IA.
[23] Cfr., ad es., cons. 81 e art. 8, § 2 del Regolamento IA.
[24] In argomento, v. A. MANTALERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, n. 54/2024, 106020.

valutazione d'impatto sulla protezione dei dati (*data protection impact assessment* - DPIA) di cui all'art. 35 GDPR[25];

c) Frizione/Estensione della base legale per l'esenzione: in altri casi ancora, il Regolamento IA introduce degli allentamenti alla normativa europea di protezione dei dati personali, sul presupposto che la scrupolosa osservanza della seconda potrebbe essere di ostacolo al perseguimento di finalità di interesse pubblico egualmente meritevoli di tutela. E così, ampliando lo spettro delle deroghe contemplate dall'art. 9(2) GDPR, il Regolamento IA aggiunge una base legale espressa per il trattamento di dati sensibili, nell'ipotesi in cui il loro trattamento sia necessario "*al fine di garantire il rilevamento e la correzione delle distorsioni* [n.d.r. "*suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future*"] *in relazione ai sistemi di IA ad alto rischio*", e sempre che siano rispettate sei condizioni cumulative dettagliate alle lettere *a)-f)* del medesimo paragrafo[26]. Con una logica non dissimile, il Regolamento IA regola, in senso ampliativo, l'"*ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico*"[27].

2. La *governance* europea dell'IA e i criteri direttivi per la *governance* nazionale

Il Capo VII del Regolamento IA è dedicato alla "*Governance*".

Si prevede, in primo luogo, l'istituzione dell'Ufficio AI presso la Commissione[28], già stabilito prima dell'entrata in vigore del Regolamento[29]. La scelta di istituire un Ufficio interno alla Commissione, in luogo di un'Agenzia o Autorità indipendente europea, potrebbe avvalorare la lettura secondo cui, anche a livello unionale, l'applicazione del Regolamento IA presenta riflessi di *policy*, non essendo, cioè, del tutto scevra da tratti di politicità, nel senso lato del termine. Da altri documenti ufficiali si evince chiaramente, del resto, l'impatto stimato dell'IA sulla competitività dell'Unione[30]. L'Ufficio ha principalmente funzioni

[25] Così l'art. 27, § 4 del Regolamento IA. A ciò deve aggiungersi che il Regolamento persegue una logica di integrazione non solo esterna (nei rapporti con il GDPR), ma anche interna (cioè tra diverse disposizioni del medesimo testo normativo). Ad esempio, si stabilisce che le informazioni che, ai sensi dell'art. 13 Regolamento IA, devono essere fornite dal *deployer* per assolvere ai doveri di trasparenza assumono valore anche agli effetti della FRIA, senza necessità, cioè, di duplicare gli adempimenti (art. 26, § 9 del Regolamento IA).

[26] Art. 10, § 5 del Regolamento IA.

[27] *Ivi*, art. 59.

[28] *Ivi*, art. 64.

[29] Decisione C(2024) 390 final del 24 gennaio 2024.

[30] Per farsi un'idea della posta in gioco si rinvia al Rapporto presentato dalla Corte dei conti europea il 29 maggio 2024 e approvato dal Consiglio il 5 novembre 2024, dal titolo "*EU artificial intelligence ambition – Stronger governance and increased, more focused investment essential going forward*" (ECA Special Report No 8/2024).

di supporto e consulenza, ma assume anche compiti di vigilanza diretta in riferimento ai modelli di IA per finalità generali (*general purpose artificial intelligence* - GPAI)[31]. Al di fuori di questa ipotesi, il Regolamento prevede l'integrale decentramento, invece, dell'attività di *enforcement* sugli Stati membri[32].

Si prevede, poi, l'istituzione di un Consiglio europeo per l'intelligenza artificiale, che fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del regolamento. Esso è composto di un rappresentante per Stato membro e vi partecipano, senza diritto di voto, l'Ufficio IA e il Garante europeo dei dati personali (*European Data Protection Supervisor* – EDPS)[33]. Chiudono il cerchio il Forum consultivo, che dà accesso a una selezione equilibrata di *stakeholder*[34], e i Gruppi di esperti scientifici indipendenti[35], entrambi volti a favorire l'ingresso di conoscenze e competenze, ma anche di interessi privati e sociali, nella fase di "messa a terra" del Regolamento.

Per quanto concerne la *governance* nazionale, si prevede che ciascuno Stato membro istituisca o designi come autorità competenti almeno un'Autorità di notifica e un'Autorità di vigilanza del mercato. Tali autorità esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del Regolamento[36].

Sussiste una sola riserva esplicita di competenza, ed è in favore del Garante per la protezione dei dati personali ("GPDP"). In particolare, nella misura in cui i sistemi di IA ad alto rischio nel campo della biometria "*sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio* [concernenti "*attività di contrasto*", "*migrazione, asilo e gestione del controllo delle frontiere*" e "*amministrazione della giustizia e processi democratici*"]*, gli Stati membri designano come autorità di vigilanza … le autorità di controllo competenti per la protezione dei dati*"[37].

Al contempo, il Regolamento pone enfasi sull'importanza che l'Autorità di vigilanza, se differente da quella di protezione di diritti fondamentali, stabilisca un effettivo coordinamento con quest'ultima.

Invero, "*le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali … in relazione all'uso dei sistemi di IA ad alto rischio … hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati entro i*

[31] Art. 88 del Regolamento IA.
[32] L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista trimestrale di diritto pubblico*, n. 4/2022, 1110-12.
[33] Art. 65 del Regolamento IA.
[34] *Ivi*, art. 67.
[35] *Ivi*, art. 68.
[36] *Ivi*, art. 70.
[37] *Ivi*, art. 74, § 8.

limiti della loro giurisdizione"[38]. Si aggiunge che "*qualora la documentazione … non sia sufficiente per accertare un'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità pubblica o l'organismo pubblico* [per la protezione dei diritti fondamentali] *può presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici. L'autorità di vigilanza del mercato organizza le prove coinvolgendo da vicino l'autorità pubblica o l'organismo pubblico richiedente entro un termine ragionevole dalla richiesta*"[39].

È previsto anche un flusso informativo a senso invertito, ossia dall'Autorità di vigilanza alle autorità o organismi di protezione di diritti fondamentali. Nello specifico, "*qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti …, e coopera pienamente con essi. I pertinenti operatori cooperano, per quanto necessario, con l'autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali* [di tutela di diritti fondamentali]"[40]. Se le suddette autorità "*rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza indebito ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di rendere il sistema di IA conforme, ritirarlo dal mercato o richiamarlo*". Inoltre, "*qualora l'operatore di un sistema di IA non adotti misure correttive adeguate nel periodo* [assegnato]*, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato nazionale, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo*", dandone notifica alla Commissione. La Commissione o l'Autorità di vigilanza di un altro Stato possono opporsi alla misura provvisoria entro 3 mesi[41]. Se il sistema di IA classificato "ad alto rischio" appare "conforme", ma il procedimento congiunto appena descritto dovesse comunque evidenziare un "rischio", nei termini sopra divisati, l'Autorità di vigilanza potrebbe imporre misure e comunicarle alla Commissione. In tale ultima circostanza, però, non opererebbe il meccanismo del silenzio-assenso in caso di mancata opposizione alla misura[42].

3. Gli spazi di discrezionalità lasciati al legislatore nazionale dal Regolamento IA

L'ampia formulazione dell'art. 70 del Regolamento IA ha aperto un dibattito, tuttora in corso, su quale debba essere la *governance* nazionale dell'intelligenza artificiale più desiderabile[43].

[38] *Ivi*, art. 77, § 1.
[39] *Ivi*, art. 77, § 3.
[40] *Ivi*, art. 79, § 2.
[41] *Ivi*, art. 79, rispettivamente §§ 5 e 6.
[42] Art. 82 del Regolamento IA.
[43] Cfr., per un inquadramento generale sul tema, C. NOVELLI - P. HACKER - J. MORLEY - J. TRONDAL - L. FLORIDI, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *European Journal of Risk Regulation*, 2024, 1 ss.

Secondo quanto illustrato dall'Autorità europea per la protezione dei dati personali (*European Data Protection Board* – EDPB), risponderebbe ai criteri di razionalità e semplificazione la scelta degli Stati membri di individuare le Autorità di protezione dei dati personali quali Autorità di vigilanza ai sensi dell'art. 70, § 1 del Regolamento IA, ferma restando la necessità di dotare tali soggetti di risorse umane e finanziarie aggiuntive[44]. Ciò in quanto le Autorità di protezione dei dati personali: i) già possiedono l'*expertise* necessaria, avendo partecipato attivamente al cantiere normativo dell'*AI Act* e occupandosi, tra l'altro, di aspetti come il trattamento dei dati personali tramite decisioni completamente automatizzate e le misure di sicurezza; ii) assicurerebbero un agevole "*single contact point*" ai soggetti interessati e alle imprese vigilate[45].

A tali rilievi si aggiungono quelli mossi dal Garante privacy nazionale nella precedente Segnalazione al Parlamento e al Governo. In tale sede, il GPDP già evidenziava come la sua investitura, in vece di agenzie riconducibili all'Esecutivo, assicurerebbe i criteri di indipendenza richiesti dal Regolamento, oltre ad apparire più razionale, atteso che il Garante è l'unico soggetto nei cui confronti il Regolamento IA pone una "riserva di competenza"[46]. Inoltre, l'individuazione del Garante come Autorità di vigilanza ridurrebbe al minimo il rischio di "conflitti di competenza e duplicazione ingiustificata degli oneri amministrativi per soggetti pubblici e privati"[47].

Da ultimo, le ragioni (sia tecniche che di indipendenza) che militano a favore di un più diretto coinvolgimento delle Autorità di protezione dei dati personali nella *governance* dell'IA sono state ribadite anche nel corso del G7[48].

La posizione assunta dall'EDPB, dal Garante privacy e dalle Autorità di protezione dei Paesi G7 sembra compatibile con l'impianto generale del Regolamento IA.

Ciò non equivale a dire, però, che una scelta legislativa di segno diverso sarebbe automaticamente contraria al diritto europeo o determinerebbe, di per sé, un pregiudizio irreversibile alla protezione dei dati personali.

Secondo una tecnica ben nota al legislatore europeo, il Regolamento resta indifferente all'organizzazione interna dello Stato membro. A prescindere dagli attori istituzionali chiamati a darvi applicazione, esso si limita a pretendere che entrambe le sue anime (*product safety* e *rights based*) siano scrupolosamente osservate. In questo contesto, il legislatore nazionale resta libero di concentrare funzioni di sicurezza di prodotto e tutela di diritti fondamentali nello stesso soggetto (ad esempio, il GPDP), così come di separare le due anime del Regolamento, istituendo una nuova autorità e/o designando un'Autorità di vigilanza del

[44] EDPB, Statement 3/2024 "*on data protection authorities' role in the Artificial Intelligence Act framework*", 16 luglio 2024, § 12.
[45] *Ivi*, §§ 6 e 8.
[46] Come visto, ai sensi dell'art. 74, § 8 del Regolamento IA.
[47] Cfr. Segnalazione al Parlamento e al Governo sull'Autorità per l'i. a., doc. web 9996508 del 25 marzo 2024.
[48] *Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI* cit., rispettivamente §§ 8-11 e § 12.

mercato geneticamente versata ad occuparsi di sicurezza tecnologica (è questo il caso, evidentemente, dell'Agenzia per la Cybersicurezza Nazionale – "ACN"[49]). Nel secondo caso, resterebbero ovviamente fermi tutti i poteri del Garante privacy, nonché le specifiche regole europee dettate in punto di coordinamento interistituzionale[50]. Salvo diversamente disposto, infatti, le regole dell'ordinamento della privacy[51] sono pienamente applicabili ai trattamenti che abbiano luogo nel contesto di sistemi di IA, rispetto ai quali i Garanti (europei e nazionali) mantengono tutti i propri poteri di intervento. Ciò in quanto l'Unione intende creare, sul piano assiologico, le basi per uno sviluppo tecnologico antropocentrico.

Alla luce di quanto precede, le ragioni addotte dalle Autorità di protezione della privacy a sostegno di una propria designazione quali Autorità di vigilanza del mercato ai fini del Regolamento IA, per quanto comprensibili e, in parte, ragionevoli, non sembrano comportare, di per sé, l'illegittimità dell'eventuale scelta allocativa di segno diverso.

Argomenti del genere, dunque, meriterebbero di essere affrontati sul distinto piano dell'opportunità, dell'*institutional design* e dell'analisi economica del diritto.

Una discussione laica sul punto imporrebbe di considerare anche il rovescio della medaglia, verificando, cioè, se esistono argomenti a sostegno di un assetto differente da quello immaginato dalle Autorità della privacy. Si pensi, solo per fare alcuni esempi, a un modello binario che non coinvolga il Garante privacy o che lo coinvolga solo in parte, oppure all'istituzione *ex novo* di un'Autorità per l'IA, da sola o in affiancamento con supervisori preesistenti.

Alcuni argomenti in tal senso sembrerebbero, in effetti, esistere.

Si potrebbe ad esempio osservare che la maggior *trustworthiness* della tecnologia potrebbe esigere trattamenti di categorie sensibili di dati personali o potrebbe richiedere modalità implementative suscettibili di entrare in tensione con princìpi cardine come, ad esempio, la *data minimization*[52] o la *purpose limitation*[53]. Significativamente, almeno due norme del Regolamento IA propongono, come visto, degli allentamenti della disciplina generale dettata dal GDPR[54]. Pur assumendo un carattere circoscritto e mostrandosi rispettose, nel loro complesso, dello spirito del GDPR, questi "adattamenti" suggeriscono, su un piano più generale, che le due anime del Regolamento IA (*product safety approach* e *rights based approach*)

[49] In argomento, I. FORGIONE, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzioni tra regolazione europea e interna*, in *Diritto amministrativo*, n. 4/2022, 1113 ss.

[50] Artt. 77 e 79 del Regolamento IA, *in primis*.

[51] Oltre al GDPR, vengono in rilievo il Regolamento (UE) 2018/1725, sul trattamento di dati personali da parte di istituzioni o organismi europei, e la direttiva (UE) 2016/680, sulla protezione dei dati personali delle persone coinvolte in procedimenti penali.

[52] Art. 5, § 1, lett. *c)* del GDPR.

[53] Art. 5, § 1, lett. *b)* del GDPR.

[54] *I.e.*, gli artt. 10, § 5 e 59, cui fa richiamo l'art. 2, § 7 del Regolamento IA. Le citate previsioni rappresentano fattispecie, positivizzate, di trattamento per legittimo interesse *ex* art. 6, § 1, lett. *f)* del GDPR.

seguono, in linea di massima, una linea di convergenza, ma in talune circostanze potrebbero divergere, tanto da richiedere una previa composizione normativa. L'asse potrebbe ulteriormente spostarsi verso le ragioni di affidabilità tecnologica del prodotto se nell'equazione del bilanciamento facesse ingresso anche la variabile dell'innovazione e, più in particolare, del grado di competitività che si vuole riconoscere al modello europeo o nazionale di IA. A seconda della sensibilità dell'interprete, cioè, il punto di equilibrio potrebbe pendere verso l'innovazione o sbilanciarsi, invece, verso la protezione di diritti fondamentali. Detto in termini più compiuti: ferma restando l'incomprimibilità del diritto alla privacy, a fronte di una pluralità di opzioni ermeneutiche tutte astrattamente plausibili si potrebbe propendere, a seconda degli approcci, per soluzioni interpretative più o meno rigide.

Per altro profilo, non deve trascurarsi il diverso scenario in cui si registrino frizioni applicative tutte interne alla componente *rights based* del Regolamento IA. Come si vedrà[55], in astratto un determinato utilizzo di un modello di IA potrebbe andare a beneficio di un diritto fondamentale comprimendone un altro. Per fare un esempio, un accordo tra il legittimo titolare dei diritti di sfruttamento economico di un diritto di proprietà intellettuale e uno sviluppatore di sistemi di IA generativa che utilizzano *large language models* (LLM) potrebbero essere di mutuo interesse, se funzionale all'affinamento della tecnologia sottostante e alla contestuale protezione e valorizzazione del diritto d'autore, che pure rientra nel catalogo dei diritti fondamentali[56]. Tuttavia – lo si vedrà nel seguito – un simile accordo potrebbe anche sollevare criticità in punto di trattamento di dati personali. Criticità delle quali le parti dovrebbero tener conto, allora, nella relativa DPIA e FRIA.

Trattandosi di un discorso complesso e plurisfaccettato, la discussione potrebbe trarre giovamento dall'illustrazione di alcuni casi di studio[57].

Seguirà, quindi, la succinta descrizione del d.d.l. n. 1146[58] e un raffronto con le scelte compiute o in corso di definizione in altri ordinamenti giuridici[59], per concludere con una breve riflessione sui correttivi che, a giudizio di chi scrive, sarebbe auspicabile apportare al testo legislativo[60].

4. La saga OpenAi come dimostrazione vivente della pluralità di approcci possibili all'IA

L'intelligenza artificiale generativa può rappresentare un valido caso di studio per saggiare la cennata tensione tra sicurezza/competitività e diritto fondamentale, o tra diversi diritti fondamentali.

[55] *Infra* § 5.
[56] Art. 17, § 2 CDFUE.
[57] *Infra* § 4.
[58] *Infra* § 5.
[59] *Infra* § 6.
[60] *Infra* § 7.

In alcuni commenti si è osservato che l'applicazione troppo stringente del principio di limitazione delle finalità dovrebbe misurarsi con la circostanza che, in sistemi di questo genere, gli usi successivi sono di norma molteplici (raccolta di dati/addestramento/validazione/*testing*)[61]. Nei medesimi contributi si è altresì auspicato che, in conformità con gli orientamenti della Commission nationale de l'informatique et des libertés (CNIL), il principio di minimizzazione dei dati personali venga applicato nella fase *post-training*, e non in quella di *pre-training*. In questo contesto, si è sostenuto che la base giuridica più appropriata per il trattamento di dati personali ad opera di sistemi IA sarebbe quella del legittimo interesse *ex* art. 6, § 1, lett. *f)* del GDPR[62], sempre che ne siano integrati presupposti e condizioni[63]. Seguendo questa linea interpretativa, cioè, vi sarebbe un legittimo interesse al trattamento del dato personale per assicurare la "sicurezza" e "affidabilità" del sistema di IA[64], specie quando entrino in gioco interessi pubblici qualificati. Per contro, un'Autorità di controllo potrebbe essere incline ad adottare una linea più rigorosa, se rispettosa dei princìpi di proporzionalità e ragionevolezza.

La prassi decisionale del Garante privacy italiano in materia di IA generativa sembrerebbe favorire tale ultima impostazione.

Già a marzo 2023, con più di un anno di anticipo sull'entrata in vigore del Regolamento IA, il GPDP ha disposto in via di urgenza la limitazione provvisoria del trattamento, ai sensi dell'art. 58, § 2, lett. *f)* del GDPR, nei confronti di OpenAI L.L.C., società statunitense sviluppatrice del prodotto "ChatGPT", oggi definibile, ai sensi del Regolamento IA[65], come "*sistema di IA per finalità generali*"[66]. Ciò – si noti – proprio sul presupposto dell'"*assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT*", nonché dell'"*assenza di qualsivoglia verifica dell'età degli utenti in relazione al servizio ChatGPT*"[67]. Il successivo 11 aprile il Garante ha sospeso l'efficacia del citato provvedimento interinale e ordinato, ai sensi dell'art. 58, § 2, lett. *d)* del GDPR, *inter alia*, una serie di miglioramenti informativi, nonché ingiunto "*la modifica della base giuridica del trattamento dei*

[61] Cfr. E. DROUARD - O. KUROCHKINA - R. SCHLICH - D. OZTURK, *The Interplay between the AI Act and the GDPR: Part II – Compliance Challenges for AI Systems That Use Personal Data*, in *AIRe*, n. 3/2024, 297 ss. Per una guida sulle principali sfide della Generative AI alla privacy, cfr. EDPS, *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*, 3 giugno 2024.

[62] Cfr. CNIL, *Relying on the legal basis of legitimate interests to develop an AI system*, Sheet No. 8, 2 luglio 2024, ma v. anche UK ICO, *Consultation series on generative AI and data protection*. Come noto, ai sensi dell'art. 21(1) GDPR, "*l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, letter*[a] *f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*".

[63] Sui quali, da ultimo, v. le EDPB Draft Guidelines n. 1/2024 "*on processing of personal data based on Article 6(1)(f) GDPR*", Versione 1.0, poste in consultazione pubblica l'8 ottobre 2024.

[64] Arg. *ex* conss. nn. 49 e 71 GDPR.

[65] Segnatamente, ai sensi dell'art. 3, n. 66.

[66] Cfr., per la disciplina operativa, il Capo V, artt. 51 e ss.

[67] Provv. n. 112 del 30 marzo 2023, doc. web n. 9870832, ratificato dal Collegio nell'adunanza dell'8 aprile 2023.

dati personali degli utenti ai fini dell'addestramento algoritmico, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse in relazione alle valutazioni di competenza della società in una logica di accountability"[68].

Tale azione ha indotto, il 13 aprile 2023, l'EDPB a istituire una *task force* dedicata al servizio ChatGPT[69].

Con comunicato stampa del 29 gennaio 2024 il GPDP ha reso noto di aver notificato a OpenAI l'atto di contestazione per aver violato, sotto molteplici profili, la normativa in materia di protezione dei dati personali[70]. L'istruttoria – si chiarisce nel comunicato – terrà conto degli orientamenti espressi dalla *task force*, che tuttavia non vincolano l'*enforcer* nazionale.

A maggio 2024 la *task force* istituita dall'EDPB ha prodotto un *interim report*[71]. Il suddetto Report, per quanto qui di interesse, non sembra opporsi aprioristicamente a un trattamento – quantomeno nelle fasi prodromiche di raccolta/*web-scraping*; *pre-processing*/*filtering*; e *training* – per legittimo interesse *ex* art. 6, § 1, lett. *f)* GDPR, nella misura in cui vengano adottati opportuni accorgimenti tecnici, come ad esempio "*technical measures, defining precise collection criteria and ensuring that certain data categories are not collected or that certain sources (such as public social media profiles) are excluded from data collection*", o "*measures … to delete or anonymise personal data that has been collected via web scraping before the training stage*"[72]. Siccome un'analisi individuale dei dati raccolti sarebbe di fatto impossibile, il *data controller* dovrebbe però dotarsi quantomeno di meccanismi di filtro diretti a espungere dal *dataset* dati sensibili *ex* art. 9, § 1 GDPR, sempre che non ricorrano le condizioni di cui al § 2 del medesimo articolo[73]. Per quanto concerne gli *input* forniti attivamente dal *data subject* attraverso la maschera di *prompt*, il trattamento *ex* art. 6, § 1, lett. *f)* GDPR potrebbe ritenersi ammissibile, ma solo a fronte di un'informativa molto chiara[74]. Nel diverso caso di raccolta tramite *web scraping* di dati personali provenienti da soggetti passivi che non facciano un utilizzo attivo del servizio ChatGPT, invece, l'eccezione all'informativa di cui all'art. 14, § 5, lett. *b)* del GDPR potrebbe trovare applicazione[75].

Se il Garante, come inizialmente preannunciato nei Comunicati stampa, dovesse tener conto delle linee direttrici elaborate dalla *task force*, potrebbe esservi spazio per uno sviluppo antropocentrico e, al contempo, tecnologicamente sostenibile dei servizi oggetto di indagine[76].

---

[68] Provv. n. 114 dell'11 aprile 2023, doc. web n. 987470.
[69] Cfr. https://www.edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.
[70] *ChatGPT: Garante privacy, notificato a OpenAI l'atto di contestazione per le violazioni alla normativa privacy*, doc. web n. 9978020.
[71] *Report of the work undertaken by the ChatGPT Taskforce*, 23 maggio 2024.
[72] Report cit., § 17.
[73] *Ivi*, § 19.
[74] *Ivi*, §§ 21-22, ove il riferimento all'informativa di cui all'art. 14 del GDPR.
[75] *Ivi*, § 27.
[76] Nelle more, potrebbero altresì sopraggiungere le nuove Linee guida dell'EDPB in materia di legittimo interesse, delle quali pure il Garante dovrà, in caso, tener conto (EDPB, Draft Guidelines n. 1/2024 cit.).

Non è chiaro, in questo stadio, come evolverà la vicenda. I successivi interventi del Garante sembrano invero mostrare, a prima lettura, un approccio più vigoroso rispetto a quanto ipotizzato nel citato *preliminary report* della *task force* costituita in seno all'EDPB, non essendo peraltro chiaro se tale approccio rifletta la posizione dell'EDPB o meno.

In primo luogo, il GPDP ha aperto un nuovo filone di indagine in relazione al modello "Sora" sviluppato da OpenAI, in grado, secondo quanto annunciato dallo sviluppatore, di creare scene dinamiche, realistiche e fantasiose, partendo da poche istruzioni testuali[77].

In secondo luogo, il Garante privacy ha inviato un avvertimento, ai sensi dell'art. 58, § 2, lett. *a)* del GDPR, nei confronti di OpenAI e GEDI Gruppo Editoriale S.p.A. in riferimento a un accordo siglato negli Stati uniti il 24 settembre 2024. In forza di tale accordo, una mole ingente di contenuti degli editori coinvolti[78] sarebbe utilizzata da OpenAI per consentire agli utenti del servizio ChatGPT di fare ricerche in tempo reale di notizie di attualità, con contestuale fornitura di un riassunto – elaborato da sistemi di gen-AI – e del *link* diretto alla pertinente notizia. Inoltre, tutti i contenuti editoriali verrebbero utilizzati da OpenAI anche per migliorare i propri servizi e addestrare i propri algoritmi. Secondo il Garante, l'accordo sarebbe stato concluso sulla base di una DPIA carente e potrebbe violare gli artt. 9, 10, 13 e 14 del GDPR[79]. La posizione del Garante sembra essere stata in qualche modo anticipata dall'intervento di un suo componente pubblicato lo scorso maggio. Vi si legge che mentre alcuni editori, come il New York Times, hanno intentato causa contro OpenAI dopo mesi di trattative infruttuose, "altri editori … raggiungono accordi di licenza milionari con le fabbriche degli algoritmi e risolvono o, meglio, prevengono ogni questione a monte, moltiplicando gli utili e le forme di sfruttamento sui propri archivi che si rivelano utili e protagonisti di un mercato diverso rispetto a quello dell'informazione, quello, appunto, dei contenuti destinati a rendere «intelligenti» gli algoritmi di una manciata di Corporation già divenute oligopoliste del mercato dei servizi basati sull'intelligenza artificiale generativa"[80]. Al riguardo, il componente dubita del fatto che la cessione dei diritti autorali dai giornalisti agli editori comporti anche la facoltà, per questi ultimi, di sfruttare economicamente i contenuti a fini di *training* algoritmica. Anche perché – si legge nell'intervista – "l'addestramento degli algoritmi di intelligenza artificiale generativa non

[77] *Intelligenza artificiale, il Garante privacy avvia istruttoria su "Sora" di OpenAI. Chieste alla società informazioni su algoritmo che crea brevi video da poche righe di testo*, 8 marzo 2024, doc. web n. 9991867.

[78] L'accordo si estende, in particolare, ai contenuti pubblicati sui seguenti siti: www.repubblica.it, www.lastampa.it, www.laprovinciapavese.gelocal.it, www.lasentinella.gelocal.it, www.limesonline.com, www.huffingtonpost.it, www.formulapassion.it, www.mymovies.it, www.alfemminile.com.

[79] Provv. n. 741 del 27 novembre 2024, doc. web n. 10077129.

[80] Cfr. SCORZA: *"L'IA si ciba di news: dati personali a rischio". In tutto il mondo si diffondono i contratti di licenza tra editori di giornali e big tech per lo sfruttamento commerciale dei contenuti al fine di addestrare gli algoritmi: bisogna riflettere sulle ripercussioni per i dati personali e, di conseguenza, dignità e libertà degli interessati* - Intervento di Guido Scorza, 14 maggio 2024, doc. web n. 10013837.

ha nulla a che fare con il diritto di cronaca considerato che … i contenuti generati da tali servizi sono semplicemente verosimili su base statistica e probabilistica".

5. Il D.D.L. n. 1146 e il parere preventivo reso dal GPDP

Come visto, il Regolamento IA è rimasto neutrale rispetto alla questione delle designazioni nazionali: sarebbe soddisfatto dall'individuazione del Garante privacy nazionale quale Autorità di vigilanza, ma non si oppone a priori a una *governance* nazionale dell'IA che non segua un simile schema.

In questo contesto, il 20 maggio 2024 il Governo ha sottoposto all'*iter* di approvazione parlamentare il disegno di legge n. 1146, rubricato "*Disposizioni e delega al Governo in materia di intelligenza artificiale*"[81].

Come si legge nell'AIR, il d.d.l. persegue due obiettivi generali: "1*) rafforzare la competitività italiana come obiettivo strategico nella politica economica italiana nell'ambito del contesto europeo; 2) garantire ai cittadini italiani l'uso affidabile e responsabile dell'IA, attraverso una visione antropocentrica che non solo garantisca la supervisione umana in ogni fase di sviluppo e di utilizzo dei sistemi IA, ma che garantisca, attraverso la trasparenza e l'accesso dei cittadini alle informazioni, la tutela dei diritti fondamentali*".

In punto di *governance*, l'art. 18 del d.d.l. costruisce un sistema articolato su più livelli ma, sostanzialmente, descrivibile come a trazione duale:

i) in primo luogo, l'Agenzia per l'Italia digitale (AgID), ferme restando le funzioni già attribuite, è responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale e provvede a definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA, secondo quanto previsto dalla normativa nazionale e dell'Unione europea[82];

ii) in secondo luogo, l'Agenzia per la cybersicurezza nazionale (ACN), ferme restando le funzioni già attribuite, è responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza, nonché per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di IA, secondo quanto previsto dalla normativa nazionale e dell'Unione europea[83];

iii) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di IA conformi alla normativa nazionale e dell'Unione europea, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale[84];

---

[81] Tri i primi commenti, cfr. A. PAJNO, *La* governance *dell'intelligenza artificiale tra regolamento europeo e disciplina nazionale*, in *Astrid Rassegna*, n. 13/2024, 1 ss.; C. BURELLI, *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in *Quaderni AISDUE*, n. 2/2024, 1 ss.

[82] Art. 18, comma 1, lett. *a)*.

[83] Art. 18, comma 1, lett. *b)*.

[84] Art. 18, comma 1, lett. *c)*.

iv) è istituito presso la Presidenza del Consiglio dei ministri un Comitato di coordinamento, composto dai direttori generali dell'AgID e dell'ACN e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri. Il Comitato ha il compito di assicurare il coordinamento e la collaborazione tra le Autorità nazionali per l'intelligenza artificiale e le altre pubbliche amministrazioni e autorità indipendenti[85];

v) restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali[86].

Un'interpretazione sistematica di queste previsioni induce a ritenere che se la *governance* del Regolamento IA è in mano ai soggetti istituzionali puntualmente individuati nel d.d.l., la *governance* del fenomeno IA nel suo complesso – dai contorni ben più estesi rispetto al perimetro applicativo tracciato dal Regolamento – è a geometria variabile[87].

Nel "*Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale*"[88], il Garante ha espresso un giudizio complessivamente favorevole sul d.d.l., formulando tuttavia una serie di rilievi.

Dopo aver proposto di sostituire i commi 2 e 3 dell'art. 4 – contenenti richiami alla normativa sulla protezione dei dati personali – con un articolo a sé, diretto ad affermare un "vincolo generale di conformità dei trattamenti di dati personali funzionali a sistemi di i.a. alla disciplina rilevante in materia [di privacy]", e dopo aver suggerito una serie di modifiche e integrazioni su aspetti di dettaglio, al fine di assicurare il pieno rispetto della normativa in materia di protezione dei dati personali[89], il Garante ha formulato alcune critiche costruttive in punto di *governance* istituzionale.

In primo luogo, il Garante ha chiesto di essere inserito tra i soggetti abilitati a esprimersi sulla Strategia nazionale per l'intelligenza artificiale messa a punto dalla struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali per l'intelligenza artificiale e sentiti il Ministro delle imprese e del *Made in Italy*, per i profili di

[85] Art. 18, comma 2.

[86] Art. 18, comma 3.

[87] F. BASSAN - M. RABITTI, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, in *Consumerism 2024*, Diciassettesimo rapporto annuale, *Intelligenza Artificiale e protezione dei consumatori: il ruolo delle Authorities e delle Agenzie nazionali*, 10: "Se l'agenzia designata per la vigilanza sui sistemi di IA è l'ACN, perché il profilo cardine della tutela è individuato nella sicurezza (scelta del tutto legittima e coerente con la tassonomia del Regolamento IA, che vede nella sicurezza l'obiettivo-cardine), allora la vigilanza sui sistemi di IA sarà garantita da ACN, quanto alla sicurezza, in via esclusiva. L'ACN potrebbe però anche – su richiesta – fornire assistenza e consulenza alle altre autorità, alle quali resterebbe la competenza quanto alla valutazione del precipitato dell'uso dell'IA sui mercati. Qualora l'uso di sistemi di IA abbia favorito (o addirittura consentito) comportamenti anticoncorrenziali, discriminatori, iniqui, o abbia orientato (in modo illecito o comunque non trasparente) decisioni delle imprese o dei consumatori, o ancora abbia violato il diritto alla protezione dei dati personali o il diritto all'informazione, saranno le autorità di settore competenti a valutare sia i comportamenti e gli effetti sul mercato, sia l'adeguatezza, rispetto ai mercati vigilati, dei requisiti di trasparenza e spiegabilità".

[88] Provv. n. 477 del 2 agosto 2024, doc. web n. 10043532.

[89] I rilievi toccano, in particolare, gli artt. 7-10 del d.d.l.

politica industriale e di incentivazione, e il Ministro della difesa, per gli aspetti relativi ai sistemi di IA impiegabili in chiave duale[90].

In secondo luogo, "per realizzare pienamente quella leale cooperazione tra autorità competenti prevista dall'AI Act", il Garante segnala l'utilità di un suo coinvolgimento permanente nel Comitato di coordinamento disciplinato dall'art. 18, comma 2 del d.d.l.

In terzo luogo, e per le medesime ragioni, il GPDP ritiene "opportuno integrare l'articolo prevedendo, in fine, che AgID e ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati, richiedendo altresì il parere dell'Autorità rispetto a fattispecie, al loro esame, che coinvolgano aspetti di protezione dei dati. Il Garante trasmetterà, per parte sua, elementi informativi in ordine a profili di competenza di AgID o ACN suscettibili di emergere nella trattazione di propri procedimenti".

In quarto e ultimo luogo, per ragioni di certezza del diritto il Garante chiede di esplicitare, nell'art. 22, comma 2 del d.d.l., ciò che è implicito nel Regolamento IA[91], designando cioè espressamente il medesimo soggetto come Autorità chiamata a occuparsi, per i profili di competenza, dei sistemi di IA implicanti il trattamento di dati sensibili.

6. La prospettiva di diritto comparato

Prima di trarre delle conclusioni, sembra utile esaminare i modelli organizzativi che sono stati adottati o sono in corso di valutazione in altri ordinamenti giuridici[92].

A seguito dell'AI Safety Summit ospitato a novembre 2023, il Regno Unito ha istituito la Directorate for AI Safety Institute (AISA) presso il Department for Science, Innovation, and Technology. L'AISA ha funzioni di ricerca e supporto delle P.A., con lo scopo di reclutare eccellenze, attrarre talenti e convogliare risorse al fine di formare e supportare gli *officer* delle Amministrazioni[93]. In parallelo, nel 2020 i principali *supervisor* indipendenti del Regno Unito hanno istituito, su base volontaria, il Digital Regulation Cooperation Forum (DRCF), che favorisce lo scambio di informazioni e la risoluzione congiunta di questioni intersettoriali[94].

[90] Art. 17, comma 1 del d.d.l.
[91] Artt. 74, § 8 e 77, §§ 1 e 2.
[92] L'analisi che segue è aggiornata al 4 dicembre 2024.
[93] https://www.aisi.gov.uk/.
[94] Cfr. https://www.drcf.org.uk/about-us/, da cui risulta il coinvolgimento attivo nel forum della Competition & Markets Authority (CMA), dell'Information Commissioner's Office (ICO), dell'Office of Communication (Ofcom) e della Financial Conduct Authority (FCA).

In Canada è tuttora in corso di discussione una proposta presentata a giugno 2022 che comprende, tra le altre cose, l'*Artificial Intelligence and Data Act* (AIDA)[95]. Nel testo originario, l'AIDA prevede un modello accentrato di stampo ministeriale, attribuendo la vigilanza sull'IA al Ministro competente[96], con la possibilità di designare un funzionario di alto livello del ministero, l'"*Artificial Intelligence and Data Commissioner*", con funzioni di assistenza[97].

Per quanto concerne gli Stati membri dell'Unione, solo Malta e la Spagna sembrerebbero aver portato a termine l'*iter* legislativo.

La Danimarca ha designato la Agency for Digital Government come Autorità di coordinamento della vigilanza di mercato e singolo punto di contatto, mentre rimane allo stato incerto chi rivestirà il ruolo di Autorità di notifica[98].

La Finlandia, replicando lo scema seguito per la Direttive e-Privacy e NIS, in una proposta legislativa in corso di discussione ha designato dieci Autorità di sorveglianza preesistenti, individuando la Transport and Communications Agency come singolo punto di contatto[99].

In Ungheria si dispone di poco più di una risoluzione governativa, in cui si prevede di incardinare l'Autorità di vigilanza e di notifica sotto il Ministero nazionale per l'economia[100].

In una proposta legislativa il cui *iter* parlamentare è ancora in corso la Lituania ha designato la Innovation Agency come Autorità di notifica e la Regulatory Communications Authority come Autorità di vigilanza e singolo punto di contatto[101].

Malta, come anticipato, risulta essere, assieme alla Spagna, l'unico Stato dell'Unione ad aver già designato entrambe le autorità. In particolare, la Digital Innovation Authority (MDIA) e la Information Data Protection Commission agiranno congiuntamente come Autorità di vigilanza. La prima è anche designata come Autorità di notifica, assieme con il National Accreditation Board[102].

---

95 L'AIDA costituisce la Part III della Bill C-27, recante "An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts".

96 Sez. 31.

97 Sez. 33 (1).

98 https://digst.dk/nyheder/nyhedsarkiv/2024/april/rollen-som-national-tilsynsmyndighed-med-eu-s-ai-forordning-skal-varetages-af-digitaliseringsstyrelsen/.

99 https://www.lausuntopalvelu.fi/SV/Proposal/Participation?proposalId=0e252297-c14b-4b6b-a0da-0a35756c9a90.

100 https://njt.hu/jogszabaly/2024-1301-30-22.

101 https://eimin.lrv.lt/en/structure-and-contacts/news-1/lithuania-accelerates-development-of-artificial-intelligence-by-creating-a-sandbox-to-test-the-technology/.

102 https://www.mdia.gov.mt/artificial-intelligence/, in partic. riquadro "National competent authorities".

Al momento, solo tre Stati membri, ossia Polonia[103], Romania[104] e Spagna[105] sono in procinto di optare (nei primi due casi) o hanno già optato (nel terzo caso) per l'istituzione *ex novo* di un soggetto pubblico specializzato in materia di IA.

Infine, in Belgio[106], Olanda[107] e Svezia[108] si registra una momentanea stasi legislativa accompagnata da iniziative unilaterali delle Autorità di protezione dei dati personali.

7. Alcune proposte di modifica

La breve panoramica che precede consente di isolare dal confronto internazionale alcune costanti.

In primo luogo, la scelta di affidare alcune funzioni (notifica e/o vigilanza) ad agenzie governative, condivisibile o meno, non sembra essere un tabù neanche in altri ordinamenti europei.

In secondo luogo, allo stato solo Malta sembrerebbe aver conferito all'Autorità nazionale di protezione dei dati personali i poteri (nella specie, di vigilanza sul mercato) derivanti dal Regolamento IA[109].

Tutto ciò suggerisce di astenersi da una critica frontale al modello a trazione (principalmente) duale ipotizzato nel d.d.l. n. 1146 e di concentrarsi, piuttosto, sulle possibili aree di perfettibilità della proposta legislativa.

Come ben evidenziato nel parere del Garante della privacy, il d.d.l. potrebbe (e dovrebbe) meglio articolare i doveri di coordinamento tra p.A. coinvolte, direttamente o indirettamente, nella *governance* dell'IA. Lo stesso Regolamento IA, del resto, stabilisce che "*gli Stati membri agevolano il coordinamento tra le autorità di vigilanza del mercato designate a norma del presente regolamento e altre autorità o organismi nazionali pertinenti che controllano l'applicazione … di … disposizioni del diritto dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III*"[110].

---

[103] https://www.gov.pl/web/premier/projekt-ustawy-o-systemach-sztucznej-inteligencji#:~:text=Organem%20w%C5%82a%C5%9Bciwym%20w%20tym%20zakresie,skargowe%20zako%C5%84czone%20b%C4%99dzie%20wydaniem%20decyzji., da cui si evince la designazione del Ministero per la Digitalizzazione quale Autorità di notifica.

[104] https://sgg.gov.ro/1/wp-content/uploads/2024/07/ANEXA-1-10.pdf, ove si prevede che l'istituenda Autorità cumulerà le funzioni di vigilanza e di notifica.

[105] https://espanadigital.gob.es/actualidad/jose-luis-escriva-presenta-la-nueva-sede-de-la-aesia-en-coruna-impulsando-la-supervision, da cui si ricava che l'Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), stabilita a La Coruña, concentrerà i compiti di vigilanza e notifica.

[106] Data Protection Authority of Belgium - General Secretariat, *Artificial Intelligence Systems and the GDPR A Data Protection Perspective*, settembre 2024.

[107] Autoriteit Persoonsgegevens, *Call for input - Manipulative, deceptive and exploitative AI systems. Prohibitions in EU regulation 2024/1689 (AI regulation)*, settembre 2024.

[108] Come visto, tali poteri sono stati attribuiti all'Information Data Protection Commissionin, peraltro in co-gestione con la Malta Digital Innovation Authority (MDIA).

[109] https://www.imy.se/vanliga-fragor-och-svar/vilken-myndighet-kommer-overvaka-ai-forordningen-i-sverige/.

[110] Art. 74, § 10. Sull'importanza del coordinamento, v. anche P. FALLETTA - A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto*, n. 6(1)/2024, 133.

Il faro di questa previsione – lo ha ricordato anche l'EDPB[111] – è il principio di leale collaborazione istituzionale sancito dall'art. 4, § 3 TUE, nella declinazione più pregnante che oggi conosciamo, all'indomani dalle sentenze della Corte di giustizia sul caso *Meta Platforms e al.*[112] e del Consiglio di Stato sul caso *Telepass c. AGCM*[113]. L'importanza della leale collaborazione è emersa, da ultimo, pure nel corso del G7 privacy[114] e sta affiorando sempre più anche nella letteratura scientifica[115].

Si tratta di osservazioni pienamente condivisibili e che anzi meriterebbero di essere ulteriormente sviluppate.

Come visto, il Regolamento prevede che il GPDP possa rivolgersi all'ACN per acquisire, per i profili di competenza, informazioni sui sistemi di IA ad alto rischio. Ove le informazioni non bastassero, poi, l'ACN dovrebbe ritenersi gravata, su richiesta del Garante, di un vero e proprio dovere giuridico di supporto tecnologico, consistente, nella specie, nell'obbligo di "*organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici*"[116].

Un meccanismo di questo genere appare di fondamentale importanza e potrebbe essere oggetto di estensione se si considera che le competenze del Garante restano impregiudicate per tutte le tipologie di IA, non solo quelle ad alto rischio. Sicché, non si vedono particolari ragioni, al di fuori di comprovati limiti di struttura e di risorse, per escludere la possibilità per il Garante (e altre Autorità indipendenti) di inviare "richiest[e] motivat[e]" aventi ad oggetto sistemi di IA non sottoposti alla vigilanza dell'ACN. Anche perché, nel disegno dell'Esecutivo, l'ACN dovrebbe guadagnare un'*expertise* di primo piano sulla decodifica della *black box* algoritmica. Ebbene, l'art. 18 d.d.l. non prende posizione su una simile possibilità, né dettaglia in alcun modo le modalità operative del suddetto coordinamento/avvalimento. Al pari, le deleghe legislative conferite al Governo in materia di IA non pongono princìpi e criteri direttivi sul punto[117].

Ferma restando la diretta applicabilità dell'art. 77, §§ 1 e 3 del Regolamento IA, potrebbe trattarsi di un'occasione persa. Il legislatore, ad esempio, potrebbe sforzarsi di tipizzare le conseguenze dell'immotivata inerzia serbata o del diniego opposto dall'ACN a fronte di richieste, puntualmente circostanziate, di informazione/supporto avanzate dal Garante (o altre Autorità). In parallelo, si potrebbe trarre ispirazione all'esperienza del primo pilastro dell'Unione bancaria per favorire forme assidue di distacco del personale specializzato, soprattutto dall'ACN verso il Garante, con garanzia di un comando

111 EDPB, Statement 3/2024 cit., § 11.
112 Corte di giustizia, 4 luglio 2023, C-252/21, §§ 53-63.
113 Consiglio di Stato, Sez. VI, 15 gennaio 2024, n. 497.
114 *Statement on the Role of Data Protection Authorities* cit., § 16.
115 Da ultimo, P. DE HERT - P. HAJDUK, *EU cross-regime enforcement, redundancy and interdependence. Addressing overlap of enforcement structures in the digital sphere after* Meta, in *Technology & Regulation*, n. 1/2024, 291 ss.
116 Art. 77, §§ 1 e 3 del Regolamento IA.
117 Art. 22 d.d.l. 1146.

irrevocabile per un lasso di tempo sufficientemente ampio per consentire alla risorsa umana di operare con piena indipendenza. Il che non esclude – si noti – l'opportunità (e anzi la necessità) di dotare il GPDP delle risorse umane e finanziarie idonee a fronteggiare le sfide poste dall'IA.

Una seconda osservazione, di carattere più generale, attiene alla questione metodologica dei livelli e delle sedi del coordinamento istituzionale.

Si è visto che il Regolamento IA ha un contenuto eterogeneo e, come tale, abbisogna tanto di indirizzo politico quanto di vigilanza indipendente.

I due momenti, però, dovrebbero restare quanto più possibile scissi. A garanzia di una piena e indipendente protezione dei dati personali, separati devono rimanere, allora, anche i circuiti istituzionali che li hanno in carico.

Se ne possono trarre due corollari: mentre non appare necessario, né forse desiderabile, coinvolgere il Garante della privacy nella messa a punto della Strategia nazionale sull'IA, trattandosi di attività, per l'appunto, di indirizzo politico, per ragioni eguali e contrarie non sembra sufficiente aggiungere il Garante alla platea di soggetti abilitati a sedere nel Comitato di coordinamento[118]. Qui l'operazione dovrebbe essere, forse, più radicale, nel senso che i Dicasteri dovrebbero essere espunti dal consesso, e le mura del confronto non dovrebbero essere quelle di Palazzo Chigi. La previsione sembra esser frutto, per il vero, di una trasposizione decontestualizzata dell'art. 65 del Regolamento, che istituisce il Consiglio europeo per l'intelligenza artificiale, cui prendono parte un "rappresentante", normalmente di emanazione ministeriale, per Stato membro. Ma sul piano del diritto interno il coordinamento delle *policy* è già assicurato – pare – dal procedimento composito di approvazione della Strategia nazionale[119]. E non v'è ragione di riproporre il *format* quando si tratti di gestire il coordinamento tra le Autorità designate in materia di IA e le altre Autorità indipendenti. Non appare conducente, cioè, incardinare presso la sede governativa il coordinamento, giacché coordinamento significa anche dialettica. E il sottoporre a stretta osservazione governativa l'agire interistituzionale di due Agenzie che, come detto, potrebbero forse possedere, agli effetti del Regolamento, sufficienti requisiti di indipendenza[120], ma certo non sono Autorità indipendenti, potrebbe determinare la caduta dell'impalcatura, già in sé scricchiolante[121], della *governance* nazionale tratteggiata nel d.d.l.

---

[118] Art. 18, comma 2 d.d.l. 1146.

[119] *Ivi*, art. 17.

[120] L'analisi di diritto comparato che precede mostra che diversi Stati membri stanno prendendo in considerazione il modello dell'agenzia.

[121] Si rinvia sul punto a P. OCCHIUZZI, *Intelligenza artificiale e modello di governance nazionale tra AgID, ACN e Autorità amministrative indipendenti*, in F. BASSAN - M. RABITTI (a cura di), *Consumerism 2024* cit., 17 ss., in partic. 19-21, ove si evidenzia come il modello dell'Agenzia governativa proprio sia di AgID che di ACN appaia "distonico" con le prescrizioni del Regolamento (art. 70, § 1, II periodo) e con la rilevante giurisprudenza europea (Corte di giustizia, 9 marzo 2010, *Commissione c. Germania*, C-518/07).

Alla luce di quanto precede, il coordinamento dei supervisori dovrebbe aver luogo in campo neutro e coinvolgere solo tra le Agenzie designate in materia di IA e le Autorità indipendenti maggiormente toccate dal fenomeno, tra le quali rientra, a pieno titolo, il Garante privacy. Ciò, peraltro, in continuità con quanto già avviene, in Italia, per le discipline di trasposizione del *Digital Services Act*[122] e del *Data Governance Act*[123]. In mancanza di un emendamento di questo genere, per le Autorità indipendenti non resterebbe che la strada del coordinamento volontario, sul modello di quanto già avviene nell'esperienza britannica del Digital Regulation Cooperation Forum (DRCF)[124]. Le coperture per procedere in tal senso, fortunatamente, esistono. E godono di un rango costituzionale.

[122] L'art. 49 del Digital Services Act (DSA, Regolamento (UE) n. 2022/2065) impone agli Stati membri di designare un "Coordinatore dei servizi digitali". La scelta, come noto, è ricaduta sull'Autorità per le Garanzie nelle Comunicazioni (art. 15, comma 1 D.L. n. 123/2023, conv., con modificazioni, dalla L. n. 159/2023). Si prevede, a tal fine, che "*l'Autorità garante della concorrenza e del mercato, il Garante per la protezione dei dati personali e ogni altra Autorità nazionale competente, nell'ambito delle rispettive competenze, assicurano ogni necessaria collaborazione ai fini dell'esercizio da parte dell'Autorità per le garanzie nelle comunicazioni delle funzioni di Coordinatore dei Servizi Digitali. Le Autorità possono disciplinare con protocolli di intesa gli aspetti applicativi e procedimentali della reciproca collaborazione*" (art. 15, comma 2).

[123] Nel dare attuazione al Data Governance Act (DGA, Regolamento (UE) n. 2022/868), l'Italia ha designato l'AgID quale autorità competente allo svolgimento dei compiti relativi alla procedura di notifica per i servizi di intermediazione dei dati, nonché quale autorità competente alla registrazione di organizzazioni per l'altruismo dei dati (art. 2, comma 1 d. lgs. n. 144 del 2024, attuativo, in particolare, degli artt. 13, 23 e 26 DGA). In tale contesto, si prevede che "*l'AgID opera in stretta e leale cooperazione con l'Agenzia per la cybersicurezza nazionale, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali e, a tal fine, può stipulare con gli stessi specifici accordi di collaborazione non onerosi. Gli accordi definiscono le forme e i modi di esercizio del coordinamento, anche endoprocedimentale, delle competenze, nell'ambito delle rispettive attribuzioni di AgID, del Garante per la protezione dei dati personali, dell'Agenzia per la cybersicurezza nazionale e delle altre amministrazioni competenti, in relazione alla materia trattata. Nel rispetto del principio di leale collaborazione, gli accordi prevedono forme specifiche di consultazione del Garante per la protezione dei dati personali, ogniqualvolta il procedimento amministrativo realizzato da AgID abbia implicazioni in termini di protezione dei dati*" (art. 2, comma 2). L'AgID, inoltre, deve sentire, per gli aspetti di competenza, l'ACN, l'AGCM e il GPDP prima di stabilire con proprio provvedimento le disposizioni tecniche e organizzative per facilitare l'altruismo dei dati nonché le informazioni necessarie che devono essere fornite agli interessati in merito al riutilizzo dei loro dati nell'interesse generale (art. 2, comma 3).

[124] V. *supra* § 6.