

Chi governa l'intelligenza artificiale? Autorità competenti e sfide nell'attuazione nazionale dell'*AI Act*[*]

Who Governs Artificial Intelligence? Competent Authorities and Challenges in the National Implementation of the AI Act

di *Luca Megale*[**] e *Antonio Perrucci*[***]

ABSTRACT

Il contributo affronta il tema dell'attuazione domestica del Regolamento (UE) 2024/1689 in materia di intelligenza artificiale, con specifico riferimento alla delega concernente i poteri delle autorità competenti. L'indagine muove dalla constatazione che il successo del Regolamento UE dipenderà in misura decisiva dalla capacità degli Stati membri di costruire sistemi nazionali di vigilanza effettivi, coerenti e coordinati. Il contributo esamina dunque il rischio di frammentazione istituzionale, di ipertrofia normativa e lesione della certezza giuridica per gli operatori economici. Particolare attenzione è dedicata alla configurazione dei poteri di AgID e ACN, alla necessità e alle modalità di coordinamento con le autorità settoriali e al tema del raccordo tra disciplina primaria e secondaria. L'analisi si conclude evidenziando come la prassi della clausola di invarianza di spesa risulti difficilmente conciliabile con le risorse tecniche e umane richieste alle autorità competenti dal Regolamento.

The paper addresses the Italian implementation of Regulation (EU) 2024/1689 on artificial intelligence, with specific reference to the legislative delegation concerning the powers of the competent authorities. It starts from the assumption that the success of the EU Regulation will largely depend on Member States' ability to establish effective, coherent and coordinated national oversight systems. The analysis therefore explores the risks of institutional fragmentation and regulatory hypertrophy, as well as the implications for legal certainty. Particular attention is devoted to the powers entrusted to AgID and ACN, to the need for and modalities of coordination with sectoral authorities, and to the relationship between primary and secondary legislation, including cooperation among sectoral and independent bodies. The analysis concludes by highlighting that the practice of the neutrality-of-expenditure clause appears hardly compatible with the technical and human resources required from the competent authorities under the Regulation.

---

[*] Il presente contributo è frutto di una riflessione congiunta degli autori. Tuttavia, ai soli fini dell'attribuzione, si segnala che Antonio Perrucci ha curato i parr. 1 e 2, mentre Luca Megale i parr. 3, 4 e 5.

[**] Assegnista di ricerca in Diritto amministrativo, Università LUMSA di Roma.

[***] Direttore del Laboratorio sull'ecosistema digitale (LED), Fondazione Astrid.

SOMMARIO: 1. Il contesto. – 2. Il delicato passaggio dell'attuazione e la certezza del diritto. – 3. Esiste un rischio per il coordinamento e l'uniformità interpretativa tra autorità? – 3.1. La scelta delle autorità competenti. – 3.2. Il raccordo tra AgID, ACN e le altre autorità settoriali. – 3.3. I nodi da sciogliere sui poteri delle autorità competenti. – 4. Il tema del raccordo tra disciplina primaria e secondaria. – 5. Prospettive e cenni sulla prassi dell'invarianza di spesa.

1. Il contesto

La legge italiana sull'intelligenza artificiale [1] pone le basi per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2024/1689 [2] (AI Act), ma non affronta direttamente tutte le questioni rilevanti. Viene infatti affidato al Governo il compito di adottare, entro dodici mesi, uno o più decreti legislativi volti a dare piena attuazione al Regolamento. Nel presente contributo l'attenzione è rivolta particolarmente alle disposizioni che riguardano il ruolo e i poteri delle autorità competenti e, dunque, alle sfide in termini di attuazione [3].

La delega richiede una riflessione in ordine alla possibile frammentazione delle competenze, alla portata dei poteri conferiti alle autorità nazionali e, non da ultimo, alla sostenibilità istituzionale e finanziaria del modello delineato. Il Regolamento europeo consente, infatti, agli Stati membri un certo margine di discrezionalità nella definizione dell'assetto delle proprie autorità competenti [4]. Ciascuno Stato è tenuto a designare almeno due autorità [5]: almeno una autorità notificante, incaricata della supervisione delle procedure di valutazione della conformità (*fase pre–market*), e almeno una autorità di vigilanza del mercato, responsabile del controllo successivo all'immissione in commercio (fase *post–market*). La norma unionale consente dunque di istituire anche più autorità notificanti e più autorità di vigilanza, aprendo così alla prospettiva di una pluralità di soggetti competenti in ogni Stato membro, con conseguente rischio di approcci divergenti tra gli ordinamenti nazionali. Tale elasticità strutturale, se da un lato riflette il principio di sussidiarietà e l'autonomia organizzativa degli Stati, dall'altro lato impone una particolare attenzione al coordinamento interno e alla coerenza interpretativa delle norme applicative. Attenzione che deve, allo stesso tempo, essere bilanciata con la necessità per ogni Stato membro di assicurare le competenze richieste per la salvaguardia dei diritti fondamentali interessati e già di competenza di altre autorità. La sfida non è solo recepire le norme europee, ma creare un sistema nazionale di vigilanza efficace, tecnicamente competente

[1] Legge 23 settembre 2025, n. 132, *Disposizioni e deleghe del Governo in materia di intelligenza artificiale*, GU serie generale n. 223 del 25 settembre 2025.

[2] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti […], Gazzetta ufficiale dell'Unione europea, Serie L, 12.7.2024, PE/24/2024/REV/1. I commenti della dottrina sul Regolamento sono numerosi. Si veda, *ex multis*, B. Marchetti, *La regolazione europea del mercato dell'intelligenza artificiale,* in *Rivista della Regolazione dei Mercati*, 1, 2024, 3-9.

[3] Con specifico riguardo agli artt. 20 e 24 della legge 23 settembre 2025, n. 132, *Disposizioni e deleghe del Governo in materia di intelligenza artificiale*, GU serie generale n. 223 del 25 settembre 2025.

[4] Per un'analisi sull'effettiva tendenza o meno della Commissione europea ad accentrare le funzioni amministrative, si rimanda al contributo di B. Marchetti, *L'esecuzione della regolazione digitale dell'Unione europea e il ruolo della Commissione*, in *Rivista trimestrale di diritto pubblico*, 4, 2024, 1097-1120.

[5] Art. 70, *Regolamento (UE) 2024/1689*.

ed equilibrato sul piano costituzionale. Serve una riflessione anche culturale sul controllo dell'IA, che deve unire poteri incisivi, responsabilità, trasparenza e imparzialità.

Il presente contributo si articola in quattro sezioni. La prima (par. 2) analizza il tema dell'adeguamento nazionale al Regolamento, evidenziando il rischio di ipertrofia normativa, la necessità di un'attuazione proporzionata (una criticità riconosciuta anche dal recente Omnibus sull'AI Act [6]), nonché la rilevanza in termini di certezza giuridica. L'iter dell'Omnibus digitale sull'IA è in rapida evoluzione [7]: il 13 marzo 2026 il Consiglio ha adottato il proprio mandato negoziale e il 18 marzo 2026 le commissioni IMCO e LIBE del Parlamento europeo hanno approvato la relazione congiunta con 101 voti favorevoli, proponendo termini per l'applicazione degli obblighi relativi ai sistemi ad alto rischio (2 dicembre 2027 per i sistemi di cui all'Allegato III; 2 agosto 2028 per quelli dell'Allegato I). I triloghi sono attesi per la primavera 2026 [8]. Con riferimento alla decisione di affidarsi alla delega come strumento per intervenire su un settore come quello dell'intelligenza artificiale, si rimanda a un recente contributo della dottrina [9].

La seconda sezione (par. 3) esamina i poteri di vigilanza, ispettivi e sanzionatori da riconoscere alle autorità amministrative competenti, con particolare attenzione alla scelta italiana [10] di designare l'Agenzia per l'Italia Digitale e l'Agenzia per la Cybersicurezza Nazionale. La terza (par. 4) affronta il rapporto tra disciplina primaria e secondaria, quale elemento essenziale per assicurare coerenza e coordinamento multilivello nell'attuazione del Regolamento.

Le conclusioni (par. 5) offrono una sintesi dei principali profili emersi, con una riflessione critica sulle implicazioni del principio di neutralità finanziaria incluso nel co. 6 dell'articolo. Tale previsione pone interrogativi significativi sull'effettiva capacità delle amministrazioni di adempiere ai nuovi compiti di vigilanza e coordinamento.

2. Il delicato passaggio dell'attuazione e la certezza del diritto

Il tema dell'eventuale eccesso di regolazione da parte dell'Unione europea [11] e della necessità o meno di normare l'intelligenza artificiale è costantemente

---

[6] Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica che modifica i regolamenti (UE) 2024/1689 e (UE) 2018/1139 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (*Omnibus digitale sull'IA*), 2025/0359(COD), 19 novembre 2025, par. 1.

[7] Lo stato descritto è al 19 marzo 2026.

[8] Consiglio dell'Unione europea, comunicato stampa, *Council agrees position to streamline rules on Artificial Intelligence*, 13 marzo 2026; Parlamento europeo, comunicato stampa, *MEPs support postponement of certain rules on artificial intelligence*, 18 marzo 2026; EDPB-EDPS, Joint Opinion 1/2026, cit. Si veda anche T. Marcelin, *Enforcement of the AI Act*, EPRS At a Glance, PE 785.670, marzo 2026, che evidenzia il modello ibrido di enforcement e i ritardi nella designazione delle autorità nazionali competenti.

[9] O. Pollicino e G. Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, in *Rivista di diritto dei media*, 2, 2025, 2-23.

[10] Art. 20, *Legge 23 settembre 2025*, n. 132.

[11] Nel corso degli ultimi anni, posizioni critiche sull'eccesso di intervento regolamentare della Unione europea, in particolare ma non soltanto nell'ecosistema digitale, sono state espresse da studiosi, imprese (multinazionali e non) e rappresentanti istituzionali. L'espressione "*Brussels*

trattato, sia a livello scientifico, sia mediatico, sia – infine – politico. Non ci si vuole dunque soffermare su tale aspetto, quanto più sulla delicata attenzione che il legislatore deve porre a non complicare ulteriormente le previsioni del Regolamento UE, al fine di evitare il c.d. *gold-plating* [12] e dunque un rischio di disarmonizzazione contro il mercato unico [13].

Nonostante quanto indicato dalla dottrina della Corte di Giustizia [14], secondo la quale l'uso di norme di attuazione dei regolamenti è da considerarsi generalmente improprio, la prassi è oramai differente. Vi sono infatti regolamenti che esplicitamente prevedono adeguamenti nazionali, come nel caso in trattazione, nonché la consuetudine di intervenire in caso di regolamenti contenenti previsioni vaghe [15]. Tale questione assume particolare rilievo con riguardo alla legge n. 132/2025: il legislatore italiano interviene su profili – principi generali, governance settoriale in materia di sanità, giustizia, pubblica amministrazione, lavoro – per i quali il Regolamento non conteneva espresse deleghe agli Stati membri, tralasciando al contempo i profili effettivamente delegati, quali la disciplina delle *sandboxes* regolatorie (art. 57), la specificazione dei sistemi vietati (art. 5) e il regime sanzionatorio (art. 99) [16]. Il rischio che ne deriva è duplice: da un lato, un possibile contrasto con il principio di diretta applicabilità dei regolamenti, ribadito dalla Corte di giustizia fin dalla sent. del 7 febbraio 1973, causa 39/72, e la conseguente lesione della certezza giuridica; dall'altro, un vuoto normativo proprio sui profili necessari ai fini dell'effettiva operatività del Regolamento (es. *sandboxes* e regime sanzionatorio) [17].

---

effect", coniata in termini positivi dalla giurista Anu Bradford oltre dieci anni fa, ricorre sovente, con accezione prevalentemente negativa, ad indicare la scelta dell'UE di operare solo sul versante delle regole, senza riuscire a definire politiche di sostegno alla propria industria. Le osservazioni critiche sull'impianto regolamentare europeo contenute nel rapporto Draghi sul futuro della competitività europea hanno accresciuto la platea dei critici verso l'ipertrofia dell'UE.

[12] Per una ricostruzione dell'origine del termine, si veda G. Rivellini, *Il divieto di goldplating e il problema della sua giustiziabilità in Italia*, in *Rivista trimestrale di diritto pubblico*, 3, 2021, 815 ss.

[13] K. Atthof, M. Wallgren, *Clarifying Gold-Plating: Better Implementation of EU Legislation. Board of Swedish Industry and Commerce for Better Regulation (NNR) and the Swedish Better Regulation Council (Regelrådet)*, 2012, 13, accessibile al seguente link: *nnr.se*.

[14] Corte giust. 7 febbraio 1973, causa 39/72, *Commissione c. Italia*, punto 17. Vedi anche P. Craig, G. De Búrca, *Eu Law: text, cases and materials*, Oxford University Press, 2020, 138-139.

[15] Corte giust. 12 aprile 2018, causa 541/16, *Commissione c. Regno di Danimarca*, punti 31-39.

[16] La questione è sollevata, tra gli altri, da C. Burelli, *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in *Quaderni AISDUE*, 2 2024, 237 – 266, che paragona il Regolamento sull'IA più a una direttiva che a un regolamento in senso stretto, dato il grado di armonizzazione non massimo. Si veda anche G. Gallone, *L'improcrastinabile esigenza di tracciare una via "italiana" per l'intelligenza artificiale nel procedimento amministrativo*, in *Giustiziainsieme.it*.

[17] Per un'analisi dell'iter parlamentare della legge n. 132/2025, si veda O. Pollicino, G. Muto, *La legislazione delegata in materia di intelligenza artificiale*, in *Rivista di diritto dei media*, 2, 2025, cit. Sul tema della diretta applicabilità dei regolamenti e della legittimità dell'intervento legislativo nazionale, si rinvia anche a T. Karathanasis, *The AI Act: Balancing Implementation Challenges and the EU's Simplification Agenda*, 2025, in ssrn.it, cit.

Per una lettura critica della coerenza della legge n. 132/2025 con il Regolamento UE, si v. G. De Minico, E. Palomba, M. Parente, *AI Act e legge italiana sull'intelligenza artificiale: un'armonizzazione "fin troppo perfetta"*, in *Lecostituzionaliste.it*, 20 dicembre 2025. Sulla questione della certezza giuridica, si v. O. Pollicino, G. Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, cit.

Tra i possibili rischi, l'occasione di influenzare l'implementazione del Regolamento [18], l'estensione dell'ambito di applicazione delle misure previste e l'imposizione di sanzioni o obblighi che aumentano l'onere normativo e che rendono più difficile la compliance [19]. Non a caso, è stato rivelato che almeno il 32% degli oneri amministrativi di origine unionale derivano da decisioni degli Stati membri che vanno oltre quanto richiesto dalla legislazione UE [20].

Quanto sopra descritto assume particolare rilievo rispetto a un testo complesso quale è il Regolamento UE sull'intelligenza artificiale. Si pensi, ad esempio, che il Regolamento include 1091 elementi strutturali, intesi come articoli, allegati, considerando, ecc. [21]. La complessa articolazione – nonché la difficoltà di lettura delle disposizioni che presentano numerosi richiamati interni ed esterni ad altre normative – porta ad un alto rischio di ridurre la coerenza in fase attuativa, rendendo il testo così meno efficace nel raggiungere i suoi obiettivi principali: migliorare il funzionamento del mercato interno, promuovere un'intelligenza artificiale affidabile e garantire un elevato livello di tutela della salute, della sicurezza e dei diritti fondamentali. Si potrebbe affermare che il vero successo del Regolamento risieda proprio nel modo in cui gli Stati membri ne porteranno avanti l'attuazione [22].

Oltre alla necessità per i decisori nazionali di adottare un approccio proporzionato nell'adozione di un Regolamento aperto a margini di discrezionalità, un secondo requisito fondamentale per il successo della compliance è la certezza normativa per il settore produttivo [23]. Ciò è particolarmente importante in una materia come quella dell'intelligenza artificiale, dove gli investimenti richiesti sono notevoli e su aspettative di lungo periodo – ad esempio per acquisire la potenza di calcolo necessaria all'addestramento e all'implementazione dei modelli. Favorire tali investimenti implica dunque garantire che il quadro regolatorio sia stabile e prevedibile [24]. La normativa attribuisce un ampio margine di discrezionalità alle autorità competenti, il che può anche apparire comprensibile vista la rapidità con cui la tecnologia evolve. Un tale livello di flessibilità, allo stesso

---

[18] J. Bloom-Hansen et al., *'Transposition' of EU regulations: the politics of supplementing EU regulations with national rules*, in *Journal of European Public Policy*, 30(12), 2023, 2786-2806.

[19] E. Thomann, A. Zhelyazkova, *Moving beyond (non-)compliance: the customization of European Union policies in 27 countries*, in *Journal of European Public Policy*, 24(9), 2017, 1269-1288.

[20] European Commission, *Study to analyse differences in costs of implementing EU policy: a project under DG Environment's Framework contract for economic analysis*, ENV.F.1/FRA/2010/0044, 2015, disponibile al seguente link: *ec.europa.eu*.

[21] La ricostruzione è di T. Karathanasis, *The AI Act: Balancing Implementation Challenges and the EU's Simplification Agenda*, 2025, accessibile su SSRN: *ssrn.com*.

[22] In particolare, l'esercizio su cui gli Stati membri sono chiamati a impegnarsi è orientare l'attuazione allo scopo di conseguire la *compliance* degli operatori. La questione dell'attuazione e il legame con la compliance è affrontata da M. De Benedetto, *La compliance: nozioni e problemi*, in *Liber amicorum, dedicato a M. D'Alberti*, Giappichelli, 2024, 238 ss.

[23] Ci si può riferire al concetto di *securité juridique*. Sul punto, si veda G. Corso, M. De Benedetto, N. Rangone, *Diritto amministrativo effettivo. Una introduzione*, Il Mulino, 2022, 79 ss. che richiamano anche Conseil d'État, *La securité juridique et la complexité du droit*, 2006, in particolare, 281 ss. La norma deve essere capace "capace di anticipare e prevedere, e se offre la massima chiarezza e certezza del diritto" (punto 2.2, parere del Comitato economico e sociale europeo, Una legislazione a prova di futuro, 2016).

[24] In tal senso, è importante tenere conto che l'adozione di strumenti di intelligenza artificiale da parte delle imprese italiane risulta sensibilmente in ritardo rispetto alla media europea, come testimoniato dai dati Eurostat (si veda, tra gli altri, Confindustria, *L'intelligenza artificiale per il sistema Italia*, giugno 2025).

tempo, consente di prevedere solo entro certi limiti le scelte su cui si orienteranno gli Stati membri. Le autorità pubbliche incaricate dell'attuazione dell'AI Act dovranno quindi gestire la discrezionalità loro riconosciuta in modo da salvaguardare gli obiettivi di tutela, ma senza compromettere la certezza regolatoria necessaria agli investimenti. La questione non è nuova: ogni regime normativo incorpora un certo grado di adattabilità. Tuttavia, il rischio di minare la fiducia degli investitori è maggiore nei settori emergenti, caratterizzati da rapide trasformazioni tecnologiche, da sperimentazione e da elevati costi di accesso al mercato. Ne consegue che nell'esercizio della delega si suggerisce di dare priorità alla certezza giuridica, esercitando con prudenza i poteri di estensione del campo di applicazione della legge.

L'onerosità del quadro normativo unionale, insieme alle difficoltà legate alla valutazione dei rischi e al monitoraggio continuo, si intrecciano con il rischio di frammentazione nell'applicazione delle norme. L'attuazione efficace del Regolamento UE richiederà così un notevole impegno da parte dei soggetti coinvolti, chiamati a orientarsi in un sistema normativo complesso e strettamente connesso al resto dell'ordinamento giuridico dell'Unione europea. Una delle critiche più frequenti al Regolamento generale sulla protezione dei dati (GDPR) ha riguardato proprio l'incapacità, in pratica, nel garantire un'uniformità interpretativa [25], a causa delle visioni divergenti che si sono sviluppate tra Stati membri. Parimenti, le prospettive di un successo del Regolamento sull'IA – in termini di armonizzazione, si complicano a causa del coinvolgimento di autorità nazionali di diversa natura; situazione che potrebbe portare ad una disomogeneità interpretativa.

3. Esiste un rischio per il coordinamento e l'uniformità interpretativa tra autorità?

Un tema centrale, con riguardo all'attuazione del Regolamento, riguarda i poteri delle autorità competenti. È stato anticipato, in premessa, come ogni Stato membro è chiamato, infatti, a designare una o più autorità notificanti, incaricate di gestire le procedure di valutazione della conformità dei sistemi di AI [26], nonché una o più autorità di vigilanza del mercato, competenti per l'applicazione del regolamento sui sistemi immessi sul mercato [27].

---

[25] Un esempio, con riguardo al settore pubblico, viene da A. Marra. *Obsolescenza e attualità della legge n. 241/1990 nell'era dell'amministrazione digitale*, in A. Bartolini, T. Bonetti, B. Marchetti, B.G. Mattarella, M. Ramajoli (a cura di), *La legge n. 241 del 1990, trent'anni dopo*, Giappichelli, 2021, 391, dove scrive che "il problema di individuare in concreto come declinare i principi e gli istituti del GDPR è tutt'altro che risolto in modo univoco". Per un confronto tra la struttura di enfrocement del GDPR e dell'AI Act, con le relative complessità, si vedano M. C. Pollicino, *Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa*, in *Rivista italiana di informatica e diritto*, 1, 2025, 231-256; K. Söderlund, S. Larsson, *Enforcement Design Patterns in EU Law: An Analysis of the AI Act, in Digital Society*, 3(41), 1-21.

[26] In particolare, si tratta dell'autorità nazionale "responsabile dell'istituzione e delle'secuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio" (art. 3, (19)).

[27] In particolare, è l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2024/1689. (art. 3, (26)).

3.1. La scelta delle autorità competenti

L'Italia ha identificato quale autorità di notifica l'Agenzia per l'Italia Digitale (AgID), sottoposta alla vigilanza del Presidente del Consiglio, che nomina altresì il Direttore generale dell'Agenzia. L'autorità di vigilanza del mercato è invece l'Agenzia per la cybersicurezza nazionale (ACN), con una situazione similare a quanto descritto per l'AgID: entrambe le autorità sono strettamente legate al Presidente del Consiglio o suo delegato. Una scelta similare si ritrova in Irlanda, con la competenza di autorità di vigilanza del mercato affidata al Ministero per l'impresa, il turismo e il lavoro e la Spagna che – sebbene abbia previsto un'agenzia *ad hoc* sul tema dell'intelligenza artificiale, non ne ha assicurato l'indipendenza dal Governo (a capo vi è il Ministero per la trasformazione digitale e la funzione pubblica) [28]. Diversamente, Lituania, Cipro, Slovenia e Lussemburgo hanno scelto autorità indipendenti [29]. Anche là dove si è optato per l'indipendenza, non mancano però ulteriori complessità: si va da autorità garanti per le comunicazioni (Cipro, Lituania e Slovenia) ad autorità garanti per la protezione dei dati personali (Lussemburgo) – come qualcuno aveva raccomandato per il caso italiano [30], ad autorità di salvaguardia dei diritti dei consumatori (Lettonia). Tale eterogeneità nasconde il rischio di divergenza: un'autorità con competenze primarie in materia di protezione dei dati potrebbe leggere le disposizioni in altra prospettiva rispetto ad un'autorità focalizzata sulla sicurezza dei prodotti. Lo stesso ragionamento vale per la questione dell'indipendenza o meno delle autorità pubbliche. È bene ricordare che l'indipendenza deve essere formale, ma soprattutto sostanziale, come ricordato dalla Commissione nel parere espresso riguardo alla normativa italiana [31]. La questione dell'indipendenza merita un approfondimento specifico, tanto sul piano della compatibilità con il Regolamento UE quanto su quello della sua appropriatezza sostanziale. Sul primo versante, occorre ricordare che l'art. 70, co. 1, del regolamento (UE) 2024/1689 prescrive che le autorità competenti esercitino i propri poteri "in modo indipendente, imparziale e obiettivo". Tale formulazione, pur non imponendo espressamente un'indipendenza "genetica" dal potere esecutivo – requisito che era stato previsto nella versione approvata dal Parlamento europeo nel giugno 2023 (*ex* art. 59, par. 4 *bis*) e poi espunto nei triloghi –, non può essere ridotta a un'indipendenza meramente funzionale [32]. La giurisprudenza della

---

[28] Si veda lo Statuto approvato con Real Decreto 729/2023, de 22 de agosto*, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial,* publicado en el Boletin oficial del Estado de 2 de septiembre de 2023. Sebbene l'Agenzia sia dotata di personalità giuridica pubblica e di autonomia funzionale e gestionale, non può essere qualificata come autorità pienamente indipendente dal Governo. Essa è infatti incardinata presso il Ministero per la trasformazione digitale e la funzione pubblica, tramite la Segreteria di Stato per la digitalizzazione e l'intelligenza artificiale, il cui titolare esercita altresì la presidenza dell'Agenzia. La configurazione organizzativa prescelta assicura pertanto un certo grado di autonomia tecnica e amministrativa, senza tuttavia recidere il legame strutturale e funzionale con l'Esecutivo.

[29] La lista è accessibile dal sito della Commissione europea e costantemente aggiornata: *digital-strategy.ec.europa.eu*.

[30] A. Pajno, *La governance dell'IA tra regolamento europeo e disciplina nazionale*, Astrid Rassegna 13, 24, 1 – 24. Un'analisi sulle autorità designate è offerta anche in M. Rabitti e F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendent*i, in *Federalismi.it*, 30, 2024, spec. 253.

[31] Si tratta del *Parere C(2024)7814)*. Sul punto, M. Rabitti, F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendent*i, cit.

[32] Come evidenziato da attenta dottrina, la formulazione attuale dell'art. 70 costituisce un

Corte di giustizia in materia di indipendenza delle autorità di vigilanza, maturata nel contesto della protezione dei dati personali, offre un parametro interpretativo significativo: è stato affermato che l'indipendenza funzionale non può considerarsi garantita ove l'autorità sia sottoposta a un'influenza diretta o indiretta del potere esecutivo idonea a orientarne le decisioni. Il rischio, nel caso italiano, è concreto: la nomina governativa dei vertici di AgID e ACN, la loro soggezione alla vigilanza del Presidente del Consiglio e l'assenza delle classiche garanzie di indipendenza espongono tali agenzie al rischio di "cattura regolatoria" e di usi politici dell'IA, tanto più grave in ragione della sensibilità degli interessi coinvolti – diritti fondamentali, democrazia, sicurezza pubblica. Come osservato anche dall'EDPB-EDPS nel Joint Opinion 1/2026 sull'Omnibus digitale sull'IA, il sistema di vigilanza sull'intelligenza artificiale richiede garanzie di indipendenza coerenti con quelle già riconosciute nel settore della protezione dei dati [33].

Sul piano del coordinamento settoriale, già tra i primi considerando del Regolamento [34], il legislatore europeo si affretta ad esplicitare come i compiti e i poteri delle autorità di controllo competenti in materia di protezione dei dati personali rimangano invariati. Il testo va anche oltre tale indicazione: alle autorità garanti per la protezione dei dati personali sono affidati taluni poteri specifici. A titolo esemplificativo, i garanti devono vedersi notificati tutti gli usi di sistemi di identificazione biometrica "in tempo reale" [35]; devono avere accesso alla documentazione creata a norma del Regolamento sull'IA [36] e le autorità nazionali designate devono rendere partecipi le autorità garanti per la protezione dei dati personali negli spazi di sperimentazione normativa [37], là dove sono trattati dati personali e quindi nella maggior parte dei casi (lo stesso vale per eventuali competenze di altre amministrazioni nazionali [38]). Inoltre, la valutazione d'impatto sui diritti fondamentali può integrare la valutazione d'impatto sulla protezione dei dati [39], in caso di sovrapposizione degli obblighi demandati. Viene, peraltro, specificato che un sistema di IA considerando ad alto rischio potrebbe pur sempre essere ritenuto non lecito a norma di altri atti giuridici, quale proprio la normativa in materia di protezione dei

---

compromesso al ribasso rispetto all'impostazione originaria del Parlamento europeo: v. G. De Minico, E. Palomba, M. Parente, *AI Act e legge italiana sull'intelligenza artificiale: un'armonizzazione "fin troppo perfetta"*, cit., nonché E. Sacchetto, L. Carrer (a cura di), *Garantire i diritti nell'era dell'IA*, Hermes Center/The Good Lobby, settembre 2025, spec. 14-15. In chiave comparativa, si consideri la consolidata giurisprudenza della Corte di giustizia in materia di indipendenza delle autorità di controllo nel settore della protezione dei dati personali: Corte giust. 9 marzo 2010, C-518/07, Commissione c. Germania; Corte giust. 16 ottobre 2012, C-614/10, Commissione c. Austria.

[33] EDPB-EDPS, *Joint Opinion 1/2026 on the Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, adottato il 20 gennaio 2026, spec. parr. 35-41, dove si sottolinea l'esigenza di garantire che le modifiche proposte non incidano sull'indipendenza e sui poteri delle autorità di protezione dei dati. Si veda anche N. Rangone, *The Paradoxes of the European Union's AI Regulation*, in *TheRegulatoryReview.org*, 10 marzo 2026.

[34] Considerando 10 e 157, Regolamento (UE) 2024/1689.

[35] Considerando 36, Regolamento (UE) 2024/1689.

[36] Considerando 157, come ripreso dall'art. 5, co. 6., Regolamento (UE) 2024/1689.

[37] Sul punto, si veda E. Cirone, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, *in Rivista italiana di informatica e diritto*, 1, 2025, 258-278;

[38] Art. 57, co. 10, Regolamento (UE) 2024/1689.

[39] Art. 27, co. 4., Regolamento (UE) 2024/1689.

dati personali [40]. In casi specifici [41], l'autorità di vigilanza deve dunque essere esplicitamente l'autorità garante per la protezione dei dati personali [42]. Non a caso, nonostante l'istituzione di un apposito ufficio della Commissione dedicato al Regolamento, anche l'autorità scelta per la vigilanza sulle istituzioni UE è il Garante europeo della protezione dei dati [43], che siede anche come osservatore nel Consiglio per l'IA [44]. Lo stesso Garante europeo ha raccomandato agli Stati membri di affidare il coordinamento nazionale alle autorità di protezione dei dati personali (e si era offerto anche il garante italiano con una segnalazione al Parlamento e al Governo [45]). Tale ragionamento era chiaramente connesso alla competenza che i garanti hanno già acquisito con riguardo al processo decisionale automatizzato [46].

Inoltre, sebbene non così esplicitamente, la competenza settoriale rimane anche per altre autorità pubbliche. Si pensi all'obbligo per le autorità di vigilanza di comunicare alle altre autorità, annualmente, qualsiasi informazione di possibile interesse per l'applicazione della normativa in materia di concorrenza [47] o alla competenza dell'Autorità per le garanzie nelle comunicazioni (AGCOM), in qualità di Coordinatori dei Servizi Digitali [48]. Per quanto riguarda AGCOM emerge anche un ruolo che dovrebbe essere ancora più rilevante, in virtù della natura delle piattaforme digitali quali infrastrutture su cui si sviluppano anche sistemi di IA [49]; peraltro, fortemente interessate dal trattamento dei dati.

Sono, poi, immutate le competenze che riguardano le autorità competenti in materia di tutela dei consumatori, dei servizi finanziari, della protezione dei lavoratori e sicurezza dei prodotti – temi rispetto ai quali il Regolamento sull'IA è da leggere in via complementare [50]. Forme di collaborazione e coordinamento dovranno anche interessare il rapporto con l'ANAC, in virtù della gestione affidata con riguardo alla piattaforma unica della trasparenza e alla banca nazionale dei contratti pubblici, come già richiamato dalla dottrina [51].

---

[40] Considerando 36, Regolamento (UE) 2024/1689.

[41] Si tratta, secondo l'art. 74, co. 8, Regolamento (UE) 2024/1689, dei sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e dei sistemi di IA ad alto rischio elencati nell'allegato III, punti 6, 7 e 8.

[42] O altra autorità designata secondo la direttiva (UE) 2016/680 sul trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. *Ibid*.

[43] Art. 74, co. 9., Regolamento (UE) 2024/1689.

[44] Art. 65, co. 2., Regolamento (UE) 2024/1689.

[45] Garante per la protezione dei dati personali, *Segnalazione al Parlamento e al Governo sull'Autorità per l'I.A.,* doc. web. 99964493, 25 marzo 2024.

[46] Per un'analisi dell'esperienza delle autorità di protezione dei dati personali nell'enforcement sul processo decisionale automatizzato, si veda recentemnete J. Mazur, C. Novelli, Z. Choinska, *Should Data Protection Authorities Enforce the AI Act? Lessons from EU-wide Enforcement Data*, working paper, consulabile al seguente link: *papers.ssrn.com*. Si veda, inoltre, A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 80 ss.

[47] Art. 74, co. 2., Regolamento (UE) 2024/1689.

[48] Ai sensi dell'art. 15 del d.l. 15 settembre 2023, n. 123, convertito, con modificazioni, dalla legge 13 novembre 2023, n. 159.

[49] M. Rabitti, F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, cit.

[50] Così come evidenziato dal considerando 9, Regolamento (UE) 2024/1689.

[51] M. Rabitti, F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendent*i, cit.

Per evitare disallineamenti in grado di ostacolare le imprese che intendono operare a livello europeo (in un settore quale l'IA, agli operatori economici difficilmente si può chiedere di ragionare in una prospettiva semplicemente nazionale), sarà necessario che l'attuazione della delega sia svolta in stretto contatto con la Commissione, al fine di garantire un'interpretazione uniforme delle disposizioni e una chiara ripartizione dei compiti tra le autorità nazionali.

3.2. Il raccordo tra AgID, ACN e le altre autorità settoriali

Un aspetto non chiarito dalla normativa nazionale riguarda, invece, il raccordo tra le competenze affidate ad AgID e ACN con le autorità che, secondo il Regolamento, rimangono competenti per la sicurezza dei prodotti in virtù della disciplina di armonizzazione [52]. Ad esempio, in Italia, con d.lgs. n. 157/2022 sono state individuate l'Agenzia delle Dogane e dei Monopoli e la Guardia di Finanza come autorità incaricate [53] per la conformità e sicurezza dei prodotti.

Come poi di sovente accade (è il caso anche della c.d. direttiva polizia [54] rispetto al GDPR), le attività di contrasto, gestione delle frontiere, giustizia e tutela dei processi democratici sono da affidare a specifiche autorità di contrasto [55]. Tale previsione è di rilievo, ad esempio, con riguardo ai sistemi di identificazione biometrica remota "in tempo reale" e in spazi accessibili al pubblico, ove si richiedono una valutazione d'impatto sui diritti fondamentali [56] e un'autorizzazione da parte di tali autorità [57].

Tra le criticità fondamentali, non è chiara l'interpretazione domestica delle autorità che tutelano i diritti fondamentali. L'Italia ne ha identificate solo 5 [58], mentre – ad esempio – l'Austria ne ha identificate 17 e la Spagna ben 22. Tali autorità non sono menzionate neanche in relazione al comitato di coordinamento nazionale, là dove appare peraltro particolarmente significativa l'esclusione del Garante per la protezione dei dati personali [59]. L'unica menzione attiene al generale coordinamento da assicurare con le autorità indipendenti e, in generale, con le pubbliche amministrazioni. Sul punto attenta dottrina ha messo in dubbio l'impostazione del comitato, con le autorità amministrative indipendenti che, come tali, non dovrebbero essere soggette a *coordinamento* [60].

Le basi fondamentali per creare un sistema di vigilanza e sanzionatorio efficace partono dunque da una stretta collaborazione tra le autorità designate con le altre già operanti in settori complementari. Non a caso, la disposizione

---

[52] Elencata nell'Allegato I, sezione A, Regolamento (UE) 2024/1689.

[53] A norma del Regolamento (UE) 2019/1020.

[54] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, L. 119/89, 4 maggio 2016.

[55] Art. 3, co. 45); Allegato III, co. 6, Regolamento (UE) 2024/1689.

[56] Art. 27, Regolamento (UE) 2024/1689.

[57] Considerando 34 e 35 e art. 5, 2), Regolamento (UE) 2024/1689.

[58] Si veda il sito della Commissione europea al seguente link: *digital-strategy.ec*.

[59] Secondo quanto disposto dall'art. 20, c. 3, della legge 23 settembre 2025, n. 132, il comitato è infatti composto dai direttori generali di AgID e ACN, insieme ai rappresentanti di Banca d'Italia, Consob e IVASS, in caso di questioni di competenza.

[60] M. Rabitti, F. Bassan, *L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti*, cit.

relativa alla designazione delle autorità nazionali competenti richiede alle autorità designate una competenza approfondita a livello tecnico, di protezione dei dati personali, cibersicurezza e, in termini più generali, della normativa rilevante [61].

La competenza delle autorità designate assume così particolare urgenza in un caso come quello italiano, là dove non si è optato per una diversificazione delle autorità di vigilanza su base settoriale (come consente il Regolamento, fatto salvo un punto unico di contatto nazionale [62]). Le uniche eccezioni sono quelle esplicitate dal Regolamento UE stesso. Innanzitutto, una previsione riguarda i servizi finanziari. Il testo demanda, infatti, l'adeguamento della normativa domestica al Regolamento, esplicitando la necessità di intervento – con modifiche, integrazioni e abrogazioni – in materia di servizi bancari, finanziari, assicurativi e di pagamento (i poteri di vigilanza sono affidati alla Banca d'Italia, alla CONSOB e all'IVASS [63]). Tale disposizione è imposta dal Regolamento UE, il quale affida esplicitamente la vigilanza dei sistemi di IA ad alto rischio usati da istituti finanziari alle autorità di vigilanza già operanti in tale settore [64]. La *ratio*, che avrebbe dovuto guidare forse anche la vigilanza di altri settori con maggiore coraggio da parte del Regolamento, è proprio quella di garantire coerenza e parità di trattamento rispetto alle regole e ai requisiti settoriali in materia di governance interna e gestione dei rischi [65]. Si tratta di conciliare due questioni di rilievo: da una parte, ridurre il rischio di ipertrofia dato dall'azione di molteplici amministrazioni, utile anche ai fini di semplificazione a favore di è chiamato alla *compliance*; dall'altra, assicurare una competenza trasversale dello Stato membro in materia di IA che si differenzia in base al settore specifico di riferimento e che richiede di valorizzare le competenze e i ruoli delle differenti amministrazioni. Il compito da assolvere in attuazione della legge, tutt'altro che agevole, è dunque quello di contemperare l'efficacia dell'azione amministrativa – affidandosi alla competenza delle autorità settoriali – con la necessità di rendere più agevole il contesto per gli operatori del settore – affidandosi alla supervisione e al coordinamento di un singolo punto di contatto, identificato dalla normativa in ACN.

La stringente necessità di coordinamento è fondamentale anche considerando quanto evidenziato dalla Corte di giustizia in materia di competenza condivisa e obblighi di coordinamento riguardo all'uso della normativa sulla protezione dei dati personali per violazioni di natura concorrenziale [66]. La normativa di adeguamento dovrebbe così concentrarsi, in via primaria, sulle modalità di collaborazione e sul principio di leale cooperazione [67] tra le autorità competenti in una materia così trasversale come quella dell'IA. Ciò alla luce del fatto che

[61] Art. 70, co. 3, Regolamento (UE) 2024/1689.

[62] Art. 70, co. 1, Regolamento (UE) 2024/1689.

[63] Art. 20, co. 1, legge 23 settembre 2025, n. 132.

[64] Art. 74 (6), Regolamento (UE) 2024/1689.

[65] Considerando 158, Regolamento (UE) 2024/1689.

[66] Corte giust. 4 luglio 2023, C-252/21*, Meta Platforms e a.*, punto 44 ss. Sul rapporto tra diritto antitrust e IA, si veda P. Manzini, *Intelligenza artificiale e diritto della concorrenza*, in *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, 2021, 422 ss.

[67] Sul punto, si veda S. Villani, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE*, 2, 2024, 1-20.

tale obbligo di leale collaborazione [68] non è, malauguratamente, ben affidato sul piano sovranazionale (come già specificato, è bene ricordare che, ad esempio, il garante europeo per la protezione dei dati personali partecipa solo come osservatore al Comitato europeo per l'IA [69]) e i diversi *fora* non sembrano includere garanzie di coordinamento. La storia della normativa europea sulla protezione dei dati personali rischia di apparire dunque foriera di difformità applicative al momento dell'enforcement domestico [70].

3.3. I nodi da sciogliere sui poteri delle autorità competenti

Esaurite le considerazioni relative alla necessità di coordinamento e al rischio di frammentazione [71] tra autorità competenti, è ora utile comprendere su cosa dovrebbe concentrarsi il futuro decreto legislativo relativamente ai poteri di AgID e ACN.

Iniziando dall'autorità di notifica – AgID, il Regolamento UE è poco chiaro rispetto all'indipendenza connessa all'uso di organismi di valutazione della conformità (che AgID deve designare e controllare) [72]. Si tratta di organismi terzi ai quali il Regolamento affida la valutazione della conformità dei sistemi di IA prima dell'immissione sul mercato e dunque significativamente protagonisti nei poteri loro affidati [73]. Non sono, infatti, previsti meccanismi di garanzia per evitare conflitti di interessi. In virtù delle già citate criticità di coordinamento, le quali interessano anche un approccio uniforme tra le diverse autorità di notifica dei vari Stati membri in termini interpretativi, la delega affidata al Governo dovrà impegnarsi a prevedere forme di trasparenza nel processo decisionale dell'Agenzia. Una già questionata [74] indipendenza della struttura nasconde un rischio significativo di lesione dell'obiettivo di imparzialità. La situazione rischia di aggravarsi ove l'attuazione dovesse dar seguito alla previsione del Regolamento UE, che consente di affidare la valutazione e il monitoraggio ad organismi nazionali di valutazione della conformità [75]. Peraltro, si consideri che l'organismo notificato può anche subappaltare, o affidare ad un'affiliata, compiti connessi alla valutazione della conformità, informando l'autorità di notifica [76]. Tale opzione rischia di rendere ancora meno trasparente il funzionamento degli organismi in questione. AgID avrà così un importante ruolo di supervisione sulla divergenza di interpretazione e applicazione della normativa da parte degli organismi.

Per quanto riguarda le autorità di vigilanza del mercato, queste potranno richiedere informazioni e accedere alla documentazione dei fornitori, nonché

---

[68] Sul principio di leale collaborazione come corollario di un più generale principio del giusto procedimento, si veda TAR Campania, Napoli, VIII, 10 giugno 2021, n. 3924.

[69] Art. 65, co. 2, Regolamento (UE) 2024/1689.

[70] G. De Minico, *Autorità indipendenti e algoritmi: una famiglia disfunzionale*, in *Osservatorio sulle fonti*, 2, 2021, 981 ss.

[71] Sul punto, si veda anche G. Di Cosimo, *Delegificazione e tutela giurisdizionale*, in *Quaderni costituzionali*, 2, 2002, 241 ss.

[72] Art. 28, Regolamento (UE) 2024/1689.

[73] C. Novelli, 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*, 16 (2), 2025, 566-590.

[74] A. Pajno, *La governance dell'IA tra regolamento europeo e disciplina nazionale*, cit.

[75] Come consente l'art. 28, co. 2, Regolamento (UE) 2024/1689.

[76] Art. 33, Regolamento (UE) 2024/1689.

sollecitare misure correttive, sino a indurre il ritiro di un sistema dal mercato [77]. Inoltre, tali autorità dovranno – insieme al Garante privacy – presentare una relazione annuale sull'uso di sistemi di identificazione biometrica "in tempo reale" [78], come anche ricevere valutazioni di impatto da deployer di sistemi di IA [79].

Una previsione più critica – e che deve essere approfondita in fase di adeguamento – è quella che riguarda la possibilità, per tali autorità, di autorizzare l'immissione sul mercato o la messa in servizio di sistemi di IA senza valutazione della conformità, in caso di situazioni debitamente giustificate (es. salute e sicurezza, tutela dell'ambiente e protezione della società) [80]. Non considerando l'obbligo, previsto dal Regolamento UE, di procedere all'autorizzazione senza ritardo, andrebbero introdotte forme di garanzie atte a limitare un potere poco delineato a livello sovranazionale [81]. Anche qui il coordinamento è essenziale, dato che tali poteri sono riconosciuti all'autorità di contrasto [82]. A livello sovranazionale, quale possibile garanzia, un controllo sull'attività di contrasto è svolto dalla Commissione, ma solo *ex post* [83].

Non è poi da sottovalutare e non andrebbe dimenticato in sede di attuazione della delega, il compito domestico di supportare la *compliance* e sensibilizzare sulle previsioni del Regolamento [84]. Il decreto dovrebbe così prevedere modalità con cui l'autorità può fornire alle imprese orientamenti e interlocuzioni a supporto dell'interpretazione normativa, nonché essere luogo di supporto agli obblighi di alfabetizzazione in materia di IA [85].

Sono numerosi gli obblighi informativi da parte dei fornitori a favore dell'autorità di vigilanza (ad esempio, anche in relazione all'accesso al codice sorgente del sistema di IA ad alto rischio [86]). Tali obblighi informativi, assieme ad altri profili di *compliance* ed ai costi di adozione di modelli e sistemi di IA, sono da bilanciare per non rischiare di costituire un ostacolo alla diffusione di applicazioni di IA presso le imprese. Come sono anche molteplici gli obblighi informativi per le autorità di vigilanza nazionali, a favore degli organismi pubblici nazionali e della Commissione.

I decreti di adeguamento saranno anche l'occasione per chiarire i poteri delle autorità che tutelano i diritti fondamentali, stante l'assenza di previsioni di raccordo sull'attività delle autorità designate e le autorità che tutelano i diritti fondamentali. Ad esempio, è bene ricordare che a queste ultime autorità deve essere riconosciuto il potere di richiedere qualsiasi documentazione relativa ai sistemi utile all'adempimento dei loro mandati [87].

L'attenzione del Governo dovrà, inoltre, soffermarsi su una misura – particolarmente importante – che si aggiunge ai rimedi giurisdizionali e amministrativi.

---

[77] Art. 79 e 80, Regolamento (UE) 2024/1689.

[78] Considerando 36, Regolamento (UE) 2024/1689.

[79] Considerando 96, Regolamento (UE) 2024/1689.

[80] Considerando 35, 130; art. 5, co. 2 e co. 3; art. 46, Regolamento (UE) 2024/1689.

[81] Considerando 130 e art. 46, Regolamento (UE) 2024/1689.

[82] Art. 46, Regolamento (UE) 2024/1689.

[83] Art. 46, co. 5 e 6, Regolamento (UE) 2024/1689.

[84] Considerando 160 e art. 9, Regolamento (UE) 2024/1689.

[85] Art. 4, Regolamento (UE) 2024/1689.

[86] Art. 74, co. 12, Regolamento (UE) 2024/1689.

[87] Art. 77, Regolamento (UE) 2024/1689.

Si tratta della possibilità, per qualsiasi tipo di soggetto, di segnalare violazioni delle disposizioni all'autorità di vigilanza [88]. Dovrà dunque essere delineato il raccordo con il sistema di tutela giurisdizionale e considerare la partecipazione dei soggetti interessati nell'attività di vigilanza del mercato. Sul punto, un recente policy paper ha evidenziato l'incompiutezza del regime di ricorso delineato dall'art. 85 del Regolamento, proponendo l'introduzione di un iter standardizzato per i reclami ispirato al modello del GDPR e raccomandando uniformità nella designazione delle autorità di cui all'art. 77 [89].

Per quanto attiene invece al piano sanzionatorio, il rinvio ai limiti edittali del regolamento è utile per assicurare uniformità europea, ma lascia aperto il problema della coerenza tra il diritto sanzionatorio europeo e le garanzie procedurali interne. La normativa delinea un sistema di criteri valutativi ampi e flessibili, che riconoscono alle autorità competenti un significativo margine di discrezionalità amministrativa nella determinazione della risposta sanzionatoria [90]. L'esperienza del GDPR [91] mostra che la discrezionalità nell'irrogazione delle sanzioni può produrre disomogeneità applicative tra Stati membri; per questo, sarebbe opportuno definire criteri di graduazione chiari e proporzionati. Si pensi alle previsioni che consentono di stabilire regole specifiche sull'applicabilità delle sanzioni amministrative pecuniarie nei confronti delle autorità pubbliche e degli organismi pubblici [92]. Tale previsione riflette la sensibilità verso l'autonomia costituzionale degli Stati e la differente natura giuridica degli enti pubblici, evitando un'applicazione automatica di strumenti sanzionatori concepiti principalmente per operatori privati. La questione della uniformità del trattamento tra attori pubblici e privati, e del bilanciamento tra responsabilità amministrativa e tutela del buon funzionamento della pubblica amministrazione, diviene però un tema importante nel contesto di sistemi di IA impiegati da amministrazioni pubbliche [93]. Sul punto rileva anche la necessità di intervenire sul rischio di strumentalizzazione delle esenzioni, là dove sembra esservi spazio per aggirare il regolamento in ambiti sensibili quali la pubblica sicurezza o la gestione della migrazione [94]. In questo contesto, la sorveglianza del mercato non costituisce solo una funzione tecnica, ma agisce come un meccanismo di tutela dei diritti fondamentali, supportando l'azione delle autorità nell'identificazione dei rischi e nella prevenzione di possibili abusi.

Ancora, il Regolamento consente che le sanzioni pecuniarie possano essere irrogate secondo modalità diverse a seconda dell'ordinamento nazionale, sia da autorità giudiziarie, sia da altri organismi amministrativi, a condizione che

---

[88] Art. 85, Regolamento (UE) 2024/1689.

[89] E. Sacchetto, L. Carrer (a cura di), *Garantire i diritti nell'era dell'IA. Meccanismi di ricorso e tutela dei diritti alla luce del regolamento europeo sull'intelligenza artificiale*, Hermes Center/The Good Lobby, settembre 2025, spec. 33-39.

[90] Si precisa che le sanzioni *ex* art. 99, Regolamento (UE) 2024/1689, devono essere predisposte tenendo in conto appositi orientamenti che la Commissione adotta in ossequio all'art. 96, Regolamento (UE) 2024/1689.

[91] C. Novelli et al., *A robust governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *European Journal of Risk Regulation*, cit.

[92] Art. 99, Regolamento (UE) 2024/1689.

[93] Vedi *supra*, n. 16.

[94] Il riferimento è all'apertura, senza chiari limiti, consentita dall'art. 46, Regolamento (UE) 2024/1689.

l'effetto sia equivalente [95]. Criticamente, tuttavia, la differenziazione può generare rischi di disomogeneità applicativa, soprattutto in contesti tecnologici complessi come l'IA, dove la rapidità e la competenza tecnica dell'autorità sono decisive.

L'elencazione dei criteri [96] relativi alle misure pecuniarie di carattere amministrativo – che spaziano dalla natura e gravità della violazione, alla durata, all'estensione del danno, fino alla cooperazione dell'operatore e al grado di responsabilità tecnica e organizzativa – rivelano un'impostazione di tipo "olistico", che mira a valutare la condotta non solo in termini formali, ma anche sostanziali e comportamentali. Si pensi, ad esempio, al riferimento alla finalità del sistema di IA e al numero di persone coinvolte [97]. Si introduce così una prospettiva sociale nella quantificazione della sanzione, coerente con la logica di tutela dei diritti fondamentali sottesa al regolamento. D'altro canto, criteri come la cooperazione con le autorità o la notifica volontaria della violazione incentivano modelli di compliance proattiva e trasparente, delineando una dimensione "premiale" del diritto sanzionatorio europeo. La stessa ampiezza dei criteri può, tuttavia, tradursi in disomogeneità interpretative e nel rischio di un'applicazione variabile delle sanzioni, a seconda delle capacità e delle politiche delle singole autorità nazionali. Analogo rilievo assume il richiamo ad ispezioni (anche a distanza [98]) senza preavviso e di controlli in condizioni reali [99]. Tali poteri, pur necessari per garantire un controllo effettivo su tecnologie spesso opache e dinamiche, sollevano interrogativi sul piano delle garanzie procedimentali e della tutela del segreto industriale, che dovranno essere attentamente bilanciati.

La sfida non è soltanto quella di calare le disposizioni europee nell'ordinamento domestico, ma di costruire un modello nazionale di vigilanza realmente efficace, tecnicamente attrezzato e costituzionalmente equilibrato. Ciò richiede una riflessione non solo organizzativa, ma anche culturale, sulla natura "amministrativa-tecnica" del controllo in materia di intelligenza artificiale, che deve conciliare poteri forti con responsabilità elevate, trasparenza decisionale e garanzie di imparzialità.

Va riconosciuto che la principale difficoltà nell'assicurare l'effettiva applicazione dei quadri normativi dell'Unione europea è strettamente legata alla struttura multilivello dell'UE e all'onere di attuazione in capo agli Stati membri. Onere la cui effettività dipende proprio da una corretta e tempestiva trasposizione delle norme europee nel diritto nazionale, dalla disponibilità di risorse sufficienti per la loro applicazione e l'effettivo impegno degli Stati membri nel garantire l'esecuzione delle disposizioni [100]. Una "trasposizione" che potrebbe, si ipotizza, essere anche l'occasione per rivedere l'approccio alla vigilanza del mercato. Sarebbe – come anticipato – il caso che, tramite strumenti di coordinamento, l'ACN svolgesse primariamente il suo ruolo come azione di supervisione e

[95] Art. 99, co. 9, Regolamento (UE) 2024/1689.

[96] *Ibid.*

[97] *Ibid.*

[98] Art, 74, co. 5, Regolamento (UE) 2024/1689.

[99] Art. 60, co. 6 e art. 74, Regolamento (UE) 2024/1689.

[100] M. Sholten, *EU (Shared) Law Enforcement: Who does what and how?*, in S. Montaldo, F. Costamagna, A. Miglio (a cura di). *Eu Law Enforcement. The evolution of sanctioning powers*, Routledge, 7-22, secondo cui l'applicazione da parte degli Stati membri si rivela efficace quando l'attuazione nazionale delle leggi dell'UE è corretta e tempestiva, quando gli Stati membri dispongono di risorse sufficienti per applicare le leggi e quando sono impegnati nel processo di applicazione.

orientamento, con una vigilanza quotidiana affidata invece alle autorità competenti a livello settoriale, come timidamente permette il Regolamento. Diversamente, lo spazio per conflitti di competenza appare più che plausibile.

4. Il tema del raccordo tra disciplina primaria e secondaria

La legge richiede attenzione specifica circa il raccordo tra disciplina primaria e secondaria, il quale assume particolare rilievo a livello nazionale, al fine di assicurare proprio la necessità di coordinamento e collaborazione trattata nei paragrafi precedenti. Il dialogo tra norme primarie e secondarie costituisce, infatti, il fulcro del rapporto tra indirizzo politico e amministrativo.

Si richiede di "ricorrere alla disciplina secondaria ove opportuno e nel rispetto delle competenze alle stesse spettanti [ndr, le autorità pubbliche]" [101], al fine di dare esecuzione al Regolamento europeo. L'ampiezza della disposizione, tuttavia, impone di ancorare l'azione delle autorità al rispetto dei principi di proporzionalità, trasparenza e buona amministrazione. Si tratta di una previsione significativa, onde evitare "lo spostamento di decisioni amministrativa nell'area legislativa" [102] da cui deriva il "malessere del diritto amministrativo" [103].

In questo senso, la disciplina secondaria in materia di intelligenza artificiale dovrà operare come strumento di "attuazione amministrativa qualificata", integrando il dettato legislativo con regolamenti e interventi in grado di assicurare una corretta implementazione del Regolamento europeo tra attuazione settoriale e supervisione nazionale. Si pensi, ad esempio, alla regolamentazione secondaria dei procedimenti di vigilanza nell'ambito dei mercati finanziari [104].

Il rapporto tra le due discipline assume, inoltre, un rilievo sistemico nella prospettiva del coordinamento multilivello tra diritto dell'Unione e diritto interno. Il potere regolamentare nazionale deve essere esercitato in modo da assicurare coerenza con gli atti di esecuzione e gli orientamenti adottati dalla Commissione europea.

Un ulteriore profilo dovrebbe riguardare la promozione della *compliance* e il supporto operativo per i fornitori e i potenziali fornitori di sistemi di IA, i quali – come previsto dal Regolamento [105] – sono tenuti a cooperare con le autorità competenti, seguendo i loro orientamenti e adottando misure tempestive e

---

[101] Art. 24, legge 23 settembre 2025, n. 132.

[102] S. Cassese, *La nuova discrezionalità*, in *Giornale di diritto amministrativo*, 6, 2022, 725-727.

[103] *Ibidem.*

[104] Si pensi, ad esempio, al d.m. 28 giugno 2022 sull'uso delle tecnologie digitali da parte dell'amministrazione finanziaria; al Regolamento Emittenti (Regolamento Consob n. 11971 del 14 maggio 1999 di attuazione del d.lgs. 24 febbraio 1998, n. 58 concernente la disciplina degli emittenti). Ancora, si veda Banca d'Italia, "Regolamento concernente il trattamento dei dati personali effettuato dalla Banca d'Italia nell'ambito della gestione degli esposti riguardanti la trasparenza delle condizioni contrattuali, la correttezza dei rapporti tra intermediari e clienti e i diritti e gli obblighi delle parti nella prestazione dei servizi di pagamento", G.U. del 30 marzo 2022, n. 75. Su quest'ultimo, si veda M. B. Armiento, *Prove di regolazione dell'intelligenza artificiale: il Regolamento della Banca d'Italia sulla gestione degli esposti*, in *Giornale di diritto amministrativo*, 1, 2023, 105-115. Si potrebbe far riferimento, altresì, all'art. 30 del Codice dei contratti pubblici, su cui si rimanda a B. Marchetti, *Le decisioni automatizzate (art. 30)*, in M. Clarich (a cura di), *Commentario sul Codice dei contratti pubblici*, Giappichelli, 2025, 357-371.

[105] Considerando 140, art. 57, Regolamento (UE) 2024/1689.

proporzionate per mitigare i rischi significativi per la sicurezza, la salute e i diritti fondamentali.

La costruzione di un corretto raccordo tra disciplina primaria e secondaria passa, infine, per la creazione di meccanismi di comunicazione istituzionale e partecipativa. Gli Stati membri, come previsto dallo stesso Regolamento [106], dovrebbero utilizzare canali esistenti o istituirne di nuovi per il dialogo con le PMI, le start-up, i deployer e gli innovatori, promuovendo così la prevedibilità e l'omogeneità interpretativa delle regole applicative. Tale apertura al dialogo regolatorio porta ad una logica di regolazione collaborativa come modalità di esercizio del potere fondata su partecipazione, trasparenza e responsabilità condivisa tra autorità e operatori economici.

Si è dunque dinnanzi ad una questione di equilibrio costituzionale tra legalità, autonomia amministrativa e tutela effettiva dei diritti. Una regolazione secondaria ben calibrata, coerente con i principi della buona amministrazione e della proporzionalità, costituisce la condizione per garantire che l'attuazione nazionale del Regolamento sia al contempo efficace, uniforme e rispettosa del sistema delle fonti dell'ordinamento interno, senza però risultare in un'occasione di "complessità amministrativa" [107].

5. Prospettive e cenni sulla prassi dell'invarianza di spesa

L'analisi dell'art. 24, con riguardo agli aspetti specifici che riguardano il ruolo e i poteri delle autorità competenti, conferma come l'adeguamento della normativa nazionale al Regolamento UE sull'IA costituisca un passaggio delicato e determinante per la riuscita complessiva dell'AI Act nel contesto interno. La delega al Governo impone di coniugare esigenze di effettività con quelle di coerenza e semplificazione. Il rischio è quello di una ipertrofia normativa che finisca per compromettere la chiarezza del quadro domestico e la certezza giuridica per gli operatori. L'obiettivo dovrebbe essere, invece, quello di un'"attuazione sobria", capace di valorizzare gli strumenti esistenti e focalizzata primariamente su meccanismi coordinamento e uniformità interpretativa tra le autorità competenti.

Il riparto di poteri tra le diverse autorità – AgID, ACN, Garante per la protezione dei dati personali e autorità settoriali – pone una sfida di coordinamento che non può essere risolta unicamente attraverso disposizioni di principio. Sarà la qualità dell'esercizio della delega a determinare l'effettiva funzionalità del sistema di vigilanza, in particolare rispetto alla trasparenza, all'indipendenza e alla capacità tecnica delle autorità coinvolte. In tale quadro, il raccordo tra disciplina primaria e secondaria assume un ruolo cruciale: solo un'interazione funzionale tra indirizzo politico e amministrativo, ancorato ai principi di proporzionalità e buona amministrazione, potrà evitare il rischio di un eccesso regolatorio o di una delegificazione impropria.

[106] Considerando 143, art. 70, Regolamento (UE) 2024/1689.

[107] Il riferimento è alle difficoltà gestionali e organizzative che interessano la cultura amministrativa italiana, cui recentemente ha fatto riferimento S. Cassese, *Un dazio in più: la burocrazia*, Corriera della Sera, 27 agosto 2025.

Particolarmente problematica, ma oramai comune [108], appare poi la previsione contenuta nel co. 6 della legge nazionale, che subordina l'attuazione dell'articolo all'assenza di nuovi o maggiori oneri per la finanza pubblica. La neutralità finanziaria, principio comprensibile in chiave di sostenibilità, rischia di tradursi, tuttavia, in un vincolo strutturale incompatibile con l'effettività dell'attuazione. La costruzione di un sistema nazionale di vigilanza sull'intelligenza artificiale – tecnicamente complesso, intersettoriale e ad alto contenuto specialistico – non può realisticamente prescindere da adeguate risorse strumentali ed umane. Con riguardo a queste ultime, peraltro, si segnala che la loro disponibilità sul mercato del lavoro italiano è assai limitata, se non palesemente inadeguata. Limitare tali risorse in nome della neutralità finanziaria significa, in ultima analisi, rischiare seriamente di svuotare di contenuto la stessa funzione di controllo e prevenzione che l'articolo intende presidiare. Non è da dimenticare, sul punto, che le autorità competenti devono disporre di "risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti" [109], nonché una conoscenza approfondita "delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza" [110]. Tanto è rilevante tale previsione che il Regolamento propone agli Stati membri di valutare un aggiornamento annuale dei requisiti relativi alle competenze e risorse necessarie [111].

In conclusione, la vera misura del successo della delega non sarà nella mera conformità formale al Regolamento, ma nella capacità di tradurlo in un sistema amministrativo coerente, tecnicamente attrezzato e dotato dei mezzi necessari a garantire un'applicazione uniforme e credibile delle regole europee. Solo un'implementazione effettiva, sostenuta da un adeguato investimento istituzionale, potrà evitare che l'attuazione domestica dell'AI Act si riduca a un esercizio di adempimento privo di sostanza. In questa prospettiva, è stato recentemente osservato come il modello regolatorio europeo sull'IA presenti paradossi strutturali, primo fra tutti la tensione tra la tutela dei diritti fondamentali e l'esigenza di non frenare l'innovazione, che può essere risolta solo attraverso un'attuazione domestica proporzionata e dotata di risorse adeguate [112].

---

[108] "Non si può parlare di buona amministrazione se non nel quadro del forte condizionamento operato sulle politiche di bilancio e di "riforma" tentate negli ultimi trent'anni in Italia dal vincolo esterno, dalla adozione indiscriminata della clausola di invarianza finanziaria, che ha impedito di distinguere spesa pubblica buona da quella cattiva, spese improduttive da veri investimenti sul futuro" F. Merloni, *La buona amministrazione tra responsabilità individuali e misure organizzative*, in F. Di Lascio, L. Lorenzoni (a cura di), *Politica e amministrazione tra etica, managerialità e responsabilità, atti del convegno in onore di Gianfranco D'Alessio*, RomaTre-Press, 2024, 20. La questione è affrontata, rispetto al tema dell'effettività e l'impatto sull'irrisolta ambiguità tra fiducia e sfiducia nella legge, in G. Corso, M. De Benedetto, N. Rangone, *Diritto amministrativo effettivo*, cit., 80.

[109] Art. 70, co. 3, Regolamento (UE) 2024/1689.

[110] Art. 28, co. 7, Regolamento (UE) 2024/1689, in relazione alle competenze demandate all'autorità di notifica.

[111] Art. 70, co. 3., Regolamento (UE) 2024/1689.

[112] N. Rangone, *The Paradoxes of the European Union's AI Regulation*, in *TheRegulatoryReview.org*, 10 marzo 2026. Si veda, inoltre, il quadro aggiornato della governance multilivello offerto da T. Marcelin, *Enforcement of the AI Act*, EPRS At a Glance, PE 785.670, marzo 2026.