



Il sistema di vigilanza sull'applicazione dell'*AI Act*: ognuno per sé?

Susanna Villani*

SOMMARIO: 1. Introduzione. – 2. Il sistema di vigilanza sull'applicazione dell'*AI Act* a livello nazionale. – 3. La vigilanza sull'applicazione dell'*AI Act* da parte dell'Unione: il Garante europeo per la protezione dei dati. – 4. Sistema di vigilanza e strumenti di cooperazione tra autorità. – 4.1. *Segue*: a livello intrastatale. – 4.2. *Segue*: a livello interstatale e sovranazionale. – 5. Riflessioni conclusive.

1. Introduzione

Il complessivo sistema di *governance* previsto dal regolamento sull'intelligenza artificiale (di seguito: *AI Act*) si articola su un doppio livello: quello sovranazionale e quello nazionale. Il livello sovranazionale comprende quattro nuove strutture (l'Ufficio per l'IA presso la Commissione¹, il Comitato europeo per l'IA composto da

* Ricercatrice in Diritto dell'Unione europea, *Alma Mater Studiorum* Università di Bologna. Ricerca parzialmente finanziata dal programma PNRR - M4C2 - Investimento 1.3, Partenariato Esteso PE00000013 - "FAIR - Future Artificial Intelligence Research" - Spoke 8 "Pervasive AI", finanziato dalla Commissione europea nell'ambito del NextGeneration EU Programme.

¹ L'Ufficio è già stato istituito con decisione C/2024/390 della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale. Per approfondimenti, si rinvia al contributo di F. FERRI, in questo *fascicolo speciale*.

rappresentanti degli Stati membri, l'*Advisory Forum* composto dagli *stakeholders* e il Comitato Scientifico formato da esperti scientifici scelti dalla Commissione); mentre il livello nazionale si affida ad un'autorità di notifica e ad un'autorità di vigilanza del mercato operante conformemente al reg. (UE) 2019/1020².

Il presente contributo si concentrerà specificamente sul sistema di vigilanza nazionale e sovranazionale e sui compiti attribuiti alle autorità di vigilanza sull'attuazione del regolamento successivamente all'immissione nel mercato dei sistemi di IA e, dunque, finalizzata a completare il meccanismo di controllo e verifica precedente all'utilizzo di detti sistemi; un meccanismo, questo, basato essenzialmente su obblighi a carico degli operatori privati³. Infatti, il regolamento prevede che, una volta immessi nel mercato, i sistemi di intelligenza artificiale siano monitorati da una struttura di natura pubblica per garantire l'applicazione corretta ed uniforme della normativa dell'Unione ed, eventualmente, per intervenire rapidamente in caso di rischi imprevisi.

L'obiettivo di tale analisi è duplice: tracciare gli elementi principali di detto sistema di vigilanza e indicare i principali elementi di tensione tra il rispetto dell'autonomia organizzativa degli Stati membri e le esigenze di coerenza sovranazionale nell'attuazione del regolamento da poco adottato. A tal fine, verranno innanzitutto illustrate le funzioni delle autorità di vigilanza da stabilirsi a livello nazionale (par. 2) nonché quelle del Garante europeo per la protezione dei dati quale autorità di vigilanza designata per le istituzioni dell'Unione (par. 3). Delineato il quadro complessivo dell'attività di vigilanza, si passerà ad approfondirne le principali criticità, specialmente rispetto al coordinamento tra le diverse autorità tanto a livello nazionale quanto sovranazionale (par. 4) per poi chiudere con delle riflessioni conclusive (par. 5).

² Regolamento (UE) 2019/1020, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011.

³ Ci si riferisce, nello specifico, alle procedure relative alla valutazione di conformità (*compliance assessment*) e alle valutazioni di impatto sui diritti fondamentali (FRIA) derivante dall'utilizzo dei sistemi di IA. Per commenti preliminari sulle valutazioni di conformità, si veda J. MÖKANDER, M. AXENTE, F. CASOLARI, L. FLORIDI, *Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation*, in *Minds&Machines*, 2022, p. 241 ss.

2. Il sistema di vigilanza sull'applicazione dell'*AI Act* a livello nazionale

L'art. 70 del regolamento europeo sull'intelligenza artificiale impone agli Stati membri di designare una o più autorità nazionali competenti, con funzioni di vigilanza del mercato e della sua corretta applicazione. Gli Stati membri possono decidere se creare un'autorità di controllo per l'IA *ad hoc* o affidare le relative funzioni e responsabilità ad un'autorità indipendente già esistente⁴. Ad ogni modo, come specificato al paragrafo 3 della medesima disposizione, è necessario che le autorità nazionali competenti «dispongano di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersecurity, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti».

Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Tuttavia, le autorità dovranno agire «in modo *indipendente, imparziale e senza pregiudizi*, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti nell'applicazione e attuazione del regolamento [corsivo aggiunto]»⁵. Nell'economia complessiva del regolamento, il rinvio a tali requisiti è coerente con i compiti affidati alle autorità che, pur non essendo organi giurisdizionali, avranno anche poteri investigativi e correttivi. In aggiunta, il carattere imparziale delle autorità di vigilanza è legato al principale obiettivo dell'*AI Act*, ovvero all'esigenza di promuovere un elevato livello di tutela dei diritti fondamentali che

⁴ Vale la pena anticipare che alcuni Stati membri hanno già provveduto a individuare le autorità di vigilanza, secondo diverse sensibilità: la Spagna ha costituito *ex novo* un'Agenzia apposita (AESIA), l'Olanda invece ha indicato il Garante per la *privacy*, mentre in Austria la scelta è ricaduta sull'Autorità competente in materia di telecomunicazioni.

⁵ *AI Act*, art. 70 (1).

saranno profondamente e trasversalmente toccati dai sistemi di intelligenza artificiale⁶.

Sul piano operativo, all'art. 74 dell'*AI Act*, il legislatore ha avuto premura di articolare i poteri delle autorità di vigilanza create *ex novo* rinviando esplicitamente al sistema istituito dal reg. 2019/1020 sulla vigilanza del mercato e la conformità dei prodotti⁷. Non potendo qui approfondire in modo puntuale quanto previsto da detto regolamento, basti dire che le autorità nazionali prescelte per monitorare l'immissione nel mercato dei sistemi di IA avranno sostanzialmente due tipologie di funzioni.

La prima funzione sarà essenzialmente di supporto dal momento che le autorità potranno fornire orientamenti e consulenza sull'attuazione del regolamento, in particolare in favore delle PMI, comprese le *start-up*, tenendo conto, a seconda dei casi, degli orientamenti e della consulenza del Comitato scientifico e della Commissione⁸.

La seconda funzione, ben più articolata, comprende invece la pura vigilanza. Sebbene, infatti, la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici in quanto non categorizzati come ad alto rischio, le autorità di vigilanza del mercato potranno adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conformemente al regolamento⁹. Le autorità potranno quindi chiedere ai fornitori informazioni e accedere alla documentazione, sollecitare l'adozione di misure correttive e il ritiro del sistema dal mercato qualora non conforme a quanto previsto dal regolamento.

⁶ Sul punto merita sottolineare che in Italia il confronto è particolarmente serrato proprio in riferimento al tema dell'indipendenza dell'autorità. Da una parte, infatti, il governo avrebbe l'intenzione di affidare i compiti di vigilanza all'Agenzia per l'Italia digitale e all'Agenzia per la cybersicurezza; due agenzie che, come sostenuto da più parti, difetterebbero del requisito cruciale dell'indipendenza. Dall'altra, il Garante Privacy ha rivendicato il proprio ruolo privilegiato nell'attuazione dell'*AI Act*, «in ragione della sua competenza sulle norme da applicare e delle sue caratteristiche di indipendenza. [...] Il Garante possiede infatti, già oggi, i requisiti di competenza e, assieme, indipendenza necessari per garantire un'attuazione del Regolamento coerente con l'obiettivo di garanzia di un livello elevato di tutela dei diritti fondamentali nel ricorso all'IA, sancito dall'art. 1, p. 1». Si veda, Garante per la protezione dei dati personali, Segnalazione al Parlamento e al Governo sull'Autorità per l'Intelligenza Artificiale del 25 marzo 2024.

⁷ Regolamento (UE) 2019/1020, cit., spec. artt. 11 e 14.

⁸ Per approfondimenti, si rinvia al contributo di F. FERRI, *op. cit.*

⁹ *AI Act*, artt. 79 e 80.

Fatti salvi i poteri di controllo di propria iniziativa, ai sensi dell'art. 73 dell'*AI Act* l'adozione delle menzionate misure potrebbe avvenire a seguito della ricezione di segnalazioni relative a gravi incidenti da parte dei fornitori di IA, di cui l'autorità di vigilanza dovrà informare gli organismi pubblici nazionali nonché la Commissione sulla base di quanto già previsto dagli artt. 19 e 20 del reg. 2019/1020¹⁰. Oppure, come stabilito dall'art. 85, «qualsiasi persona fisica o giuridica» che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni dell'*AI Act* potrà presentare all'autorità di vigilanza un reclamo motivato. Questa opportunità, vale la pena sottolinearlo, rappresenta un elemento estremamente positivo poiché, inserito per volontà del Parlamento europeo, si aggiunge ai rimedi giurisdizionali e amministrativi volti a dare concretezza al diritto ad un ricorso effettivo stabilito all'art. 47 della Carta dei diritti fondamentali¹¹. Ciononostante, vista le penurie di dettagli che caratterizza tanto l'art. 85 quanto il reg. 2019/1020 in ordine alla procedura sui reclami, è immaginabile che spetterà agli Stati membri stabilire le modalità di raccordo con il sistema di tutela giurisdizionale nazionale, una volta designate le autorità competenti.

Qualora le misure correttive di cui sopra non siano sufficienti, l'art. 99 introduce la possibilità per le autorità di vigilanza di adottare sanzioni pecuniarie e altre misure di esecuzione, inclusi avvertimenti e misure di natura non pecuniaria, applicabili in caso di violazione del regolamento da parte degli operatori. Mentre non si ritrovano specifiche circa la portata delle potenziali misure non pecuniarie, lasciando così liberi gli Stati di stabilire le regole di dettaglio, il regolamento è più stringente rispetto alle condizioni affinché le autorità possano infliggere sanzioni pecuniarie di carattere amministrativo. Infatti, all'art. 99 (7), è

¹⁰ *AI Act*, art. 73, par. 9-12.

¹¹ Per commenti sulla portata di tale diritto, si veda D. DOMENICUCCI, F. FILPO, *Art. 47*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGRAZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 864 ss.; G. D'AVINO, *Il diritto alla tutela giurisdizionale effettiva nell'art. 47 par. 1 della Carta dei diritti fondamentali dell'UE*, in A. DI STASI (a cura di), *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale della Carta*, Napoli, 2019, p. 151 ss.; M. BONELLI, M. ELIANTONIO, G. GENTILE (eds.), *Article 47 of the EU Charter and Effective Judicial Protection, The Court of Justice's Perspective*, Oxford, 2022.

espressamente richiesto di tenere in debita considerazione tutte le circostanze pertinenti della situazione specifica e, nel caso, di ulteriori criteri ivi menzionati. Quanto all'importo delle sanzioni pecuniarie, l'*AI Act* prevede dei massimali fissati sulla base di due riferimenti alternativi: un ammontare predeterminato oppure una percentuale del fatturato annuo globale nell'anno finanziario precedente. Si tratterebbe, quantitativamente, di € 35 milioni o del 7% del fatturato per violazioni circa l'applicazione di sistemi di IA vietati; € 15 milioni o il 3% del fatturato per violazioni degli obblighi previsti dal regolamento; e, infine, € 7,5 milioni o l'1,5% del fatturato per la comunicazione di informazioni errate¹². Tenuto conto di queste soglie, gli Stati membri dovranno stabilire sanzioni efficaci, proporzionate e dissuasive, comprese le sanzioni amministrative, e comunicarle alla Commissione¹³. In aggiunta, spetterà sempre agli Stati introdurre delle regole che definiscano in quale misura potranno essere inflitte sanzioni ad autorità pubbliche e organismi pubblici nazionali in caso di violazione degli obblighi previsti dall'*AI Act*¹⁴.

In ogni caso, l'esercizio da parte dell'autorità di vigilanza del mercato dei poteri sanzionatori dovrà essere soggetto alle garanzie procedurali previste dal diritto dell'Unione e da quello nazionale, inclusi il diritto ad un ricorso giurisdizionale effettivo e il giusto processo¹⁵. Ci si può dunque immaginare che i provvedimenti adottati dalle autorità di vigilanza possano essere sottoposti al sindacato delle Corti nazionali (e, nel caso, della Corte di giustizia tramite un rinvio pregiudiziale) nel rispetto, nuovamente, dell'art. 47 della Carta. Preme comunque precisare che la funzione sanzionatoria non è demandata in

¹² *AI Act*, art. 99, par. 3-5. Occorre segnalare che, rispetto alla proposta della Commissione, l'accordo raggiunto tra Parlamento e Consiglio ha introdotto massimali più proporzionati alle sanzioni amministrative per le PMI e le *start-up* in caso di violazione delle disposizioni dell'*AI Act*. Si veda, *AI Act*, art. 99, par. 6.

¹³ *Ibidem*, art. 71.

¹⁴ *Ibidem*, art. 99, par. 8. Occorre qui precisare che i fornitori di modelli di IA per finalità generali saranno sanzionabili direttamente dalla Commissione, *AI Act*, art. 101. Per approfondimenti, si rinvia al contributo di F. FERRI, *op. cit.*

¹⁵ *AI Act*, art. 99, par. 10. Per approfondimenti sul tema in generale, si rinvia a W. KOTSCHY, *Article 78 Right to an effective judicial remedy against a supervisory authority*, in C. KUNER ET AL. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, 2020, p. 1125 ss.; G. DI FEDERICO, *La riforma del procedimento comunitario antitrust e i diritti di difesa*, Napoli, 2008.

via esclusiva alle autorità di vigilanza che dovranno controllare sulla corretta applicazione del regolamento. Infatti, il paragrafo 9 dell'art. 99 lascia liberi gli Stati di prevedere che le sanzioni pecuniarie siano inflitte dai tribunali nazionali competenti o da altri organismi, secondo il proprio ordinamento giuridico nazionale. Dunque, in linea con l'autonomia procedurale degli Stati membri, non solo la dimensione organizzativa delle autorità di vigilanza ma anche la distribuzione dei poteri rispetto all'imposizione di eventuali sanzioni in caso di violazioni dell'*AI Act* si configura sotto un profilo scarsamente armonizzato a livello sovranazionale, se non rispetto a dei criteri minimi, e sostanzialmente affidato alle normative nazionali.

3. La vigilanza sull'applicazione dell'AI Act da parte dell'Unione: il Garante europeo per la protezione dei dati

Per quanto riguarda l'Unione europea, destinataria anch'essa delle medesime procedure di controllo dei sistemi di IA successive all'immissione nel mercato, il regolamento stabilisce che il Garante europeo per la protezione dei dati (di seguito: Garante europeo o GEPD)¹⁶ venga designato quale autorità di vigilanza del mercato competente per le istituzioni, organi e organismi dell'Unione¹⁷. Rispetto dunque alla definizione di «autorità di vigilanza del mercato» stabilita all'art. 3 (4) del reg. 2019/1020¹⁸ applicabile negli Stati membri, il «mercato» in cui il GEPD va ad esercitare il ruolo di autorità di vigilanza non è limitato ad un territorio fisico, ma si estende ad *ogni* spazio in cui il sistema di IA viene fornito da parte delle istituzioni,

¹⁶ Istituito nel 2004 e con sede a Bruxelles, il Garante europeo della protezione dei dati (GEPD) è l'autorità di controllo indipendente della protezione dei dati dell'Unione europea. I compiti del Garante sono esaustivamente elencati nel capitolo VI del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

¹⁷ *AI Act*, art. 70, par. 9. Ad eccezione, si badi bene, della Corte di giustizia, come specificato all'art. 74, par. 9.

¹⁸ Ai sensi dell'art. 3 (4) del regolamento 2019/1020, cit., «l'autorità di vigilanza del mercato è un'autorità designata da uno Stato membro a norma dell'articolo 10 quale responsabile della vigilanza del mercato nel territorio di tale Stato membro».

degli organismi e degli organi dell'Unione che rientrano nell'ambito di applicazione dell'*AI Act*¹⁹.

Quanto ai suoi compiti, il Garante europeo è chiamato a monitorare l'applicazione dell'*AI Act* e intervenire con gli strumenti attribuiti alle autorità di vigilanza nazionali. Per analogia, anche il Garante europeo potrà quindi adottare misure provvisorie per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo. Il Garante avrà poi la possibilità di acquisire i reclami dei singoli (nella veste di persone fisiche o giuridiche) previsti dall'art. 85 in caso di violazioni dell'*IA Act* da parte delle istituzioni e degli organismi dell'Unione, senza pregiudicare gli altri possibili rimedi amministrativi o giudiziari, quali ad esempio quelli avviati di fronte alla Corte di giustizia. Su questo aspetto, occorre però puntualizzare che si tratta, per l'appunto, di un'interpretazione per analogia, dal momento che l'*AI Act* non va a disciplinare specificamente la questione dei reclami da poter presentare al Garante europeo. Pertanto, sarà necessario procedere tramite un'operazione di integrazione normativa con atti già esistenti, ovvero il noto reg. 2016/679 (RGPD)²⁰ e il reg. 2018/1725²¹. Infatti, solo una lettura congiunta di questi atti può chiarire ulteriormente le competenze e le opzioni di intervento di detta autorità in materia di intelligenza artificiale. A titolo esemplificativo, ciò dovrebbe implicare che, nel silenzio dell'*AI Act*, venga esteso il diritto ad un ricorso giurisdizionale effettivo nei confronti del Garante europeo previsto all'art. 58 del reg. 2018/1725²² anche qualora questo non abbia dato seguito ad un reclamo relativo all'applicazione dell'*AI Act* o non abbia informato circa lo stato del medesimo.

¹⁹ EDPS, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments, punti 38 e 39.

²⁰ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

²¹ Regolamento (UE) 2018/1725, cit.

²² Ai sensi dell'art. 58, par. 5, del regolamento 2018/1725, cit., «L'esercizio da parte del Garante europeo della protezione dei dati dei poteri attribuitigli dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione».

Il regolamento è invece decisamente più esplicito in ordine al potere del GEPD di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione in caso di violazione delle norme previste dall'*IA Act*; un eventuale tesoretto, quello derivante dalle sanzioni, che andrà a contribuire al bilancio generale dell'Unione. L'art. 100 va a dettagliare tale potere, specificando le condizioni che dovranno essere rispettate per poter procedere con l'inflizione delle sanzioni.

Rispetto al meccanismo sanzionatorio previsto per i soggetti privati ai sensi dell'art. 99 illustrato nel paragrafo precedente, si prevede esplicitamente la sola possibilità di infliggere misure pecuniarie, peraltro particolarmente esigue rispetto a quelle imposte nei confronti degli operatori privati. Infatti, per le istituzioni dell'Unione la non conformità al divieto delle pratiche di IA di cui all'art. 5, ovvero quelle vietate, sarà soggetta a sanzioni amministrative pecuniarie fino a €1 milione e mezzo; la non conformità del sistema di IA ai requisiti o agli altri obblighi previsti dal regolamento, sarà soggetta a sanzioni fino a €750 mila. In queste circostanze, tenuto conto del pieno diritto di difesa delle parti, il Garante dovrà concedere alle istituzioni/organi dell'Unione l'opportunità di esprimersi in merito all'eventuale violazione, valutando poi la sanzione da infliggere sulla base dei criteri di cui all'art. 100, par. 1. A differenza della successiva disposizione, relativa alle sanzioni che la Commissione può adottare nei confronti di fornitori di sistemi di IA con finalità generale²³, l'art. 100 non prevede esplicitamente la possibilità per la Corte di giustizia di esaminare le sanzioni applicate dal Garante. Tuttavia, anche in questo caso, può venire in soccorso la lettura congiunta di quest'ultima disposizione dell'*AI Act* con l'art. 64 del reg. 2018/1725 che riconosce tale competenza alla Corte di giustizia, la quale, in caso di ricorso, potrebbe estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.

Ad ogni modo, non è da escludere che i poteri investigativi e di sorveglianza in capo al Garante europeo saranno ulteriormente specificati nelle future misure di esecuzione al fine di rendere operative ed efficaci le disposizioni dell'*AI Act*.

²³ *AI Act*, art. 101, par. 5. Per approfondimenti, si rinvia al contributo di F. FERRI, *op. cit.*

4. *Sistema di vigilanza e strumenti di cooperazione tra autorità*

La struttura di *governance* appena illustrata denota un tipo di vigilanza potenzialmente frammentata ed incentrata su interventi circoscritti al territorio dei rispettivi Stati membri e, nel caso del Garante europeo, alle attività svolte dalle istituzioni dell'Unione. Ciononostante, nello spazio dinamico ed interconnesso in cui si muovono i sistemi di intelligenza artificiale, le singole autorità di vigilanza potrebbero trovarsi ad interagire reciprocamente. Pertanto, occorre approfondire gli strumenti che potrebbero supportare una maggior cooperazione tra le autorità di vigilanza tanto a livello nazionale quanto a livello sovranazionale per garantire la piena applicazione del regolamento.

Nello specifico, due sono gli scenari di interazione su cui vale la pena soffermarsi. Il primo scenario è riconducibile al rapporto tra autorità di vigilanza appartenenti al medesimo Stato membro e che potrebbero vantare una competenza in ordine all'applicazione dell'*AI Act* (par. 4.1). Il secondo scenario riguarda, invece, l'interazione tra autorità di vigilanza operanti in diversi Stati membri o con il Garante europeo qualora, ad esempio, talune categorie di sistemi di IA presentino un rischio grave in due o più Stati membri oppure a livello UE (par. 4.2).

4.1. *Segue: a livello intrastatale*

Come detto, agli Stati membri è garantita la discrezionalità di indicare una o più autorità di vigilanza del mercato che provvedano a dare corretta applicazione all'*AI Act*. Tuttavia, il regolamento prevede tre eccezioni rispetto alla determinazione delle autorità competenti in ordine ai sistemi di IA ad alto rischio. La prima eccezione è indicata all'art. 74, par. 3, secondo cui, salvo diversa e motivata decisione adottata a livello nazionale, l'autorità di vigilanza del mercato per i sistemi collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, sarà

quella già designata a norma di tali atti giuridici²⁴. In secondo luogo, per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari e creditizi, l'autorità di vigilanza del mercato sarà quella responsabile della vigilanza finanziaria (art. 74, par. 6). La terza eccezione, prevista all'art. 74, par. 8, riguarda i sistemi utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e tutela dei processi democratici nonché i sistemi di IA ad alto rischio elencati nell'allegato III²⁵: in questi casi, gli Stati membri dovranno designare come autorità di vigilanza del mercato le autorità di controllo competenti per la protezione dei dati a norma del reg. 2016/679 e della dir. (UE) 2016/680 (cd. direttiva polizia)²⁶.

Le riserve di competenza espressamente previste dal regolamento sono finalizzate ad evitare che le attività di vigilanza sull'applicazione dell'*AI Act* pregiudichino la capacità delle autorità già esistenti di svolgere i loro compiti secondo quanto richiesto dalla normativa dell'Unione. In particolare, l'attribuzione di taluni poteri di vigilanza alle autorità nazionali per la protezione dei dati personali è motivata dalla stretta interrelazione tra IA e protezione dei dati; un legame che si rinviene anche nella competenza che dette autorità hanno acquisito rispetto al processo decisionale automatizzato²⁷. In effetti, l'area di

²⁴ Il regolamento si riferisce, nello specifico, alla normativa relativa ai prodotti già sottoposti a controlli nel quadro del mercato interno.

²⁵ Nel dettaglio, la disposizione fa riferimento all'utilizzo dei sistemi di IA per la raccolta di dati biometrici (Allegato III, punto 1) e ai sistemi ad alto rischio previsti nell'Allegato III, punti 6, 7 e 8. Da notare che le autorità per la protezione dei dati dovrebbero auspicabilmente presentare alla Commissione una relazione annuale sull'uso dei sistemi di identificazione biometrica 'in tempo reale'; un auspicio che, tuttavia, è previsto esclusivamente nel considerando n. 36 ma non si ritrova nel testo del regolamento.

²⁶ 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.

²⁷ Regolamento 2016/679, cit., art. 22. Per approfondimenti, F. UFERT, *AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?*, in *EP*, n. 5, 2020, p. 1087 ss.; G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, *European Parliament Study*, 2020; J. ANDRAŠKO, M. MESARČÍK, O. HAMUEÁK, *The*

tutela relativa ai dati personali è certamente una delle più interessate dalla diffusione e pervasività dei sistemi di intelligenza artificiale perché l'elaborazione, l'analisi e il trattamento di grandi quantitativi di dati sono alla base del funzionamento dell'intelligenza artificiale. Tuttavia, i diritti fondamentali che l'*AI Act* intende tutelare sono riconducibili ad un insieme più ampio, a seconda della tecnologia e dell'ambito di utilizzo. Per questo, a differenza di quanto auspicato dal Garante europeo nel parere emesso nel 2021²⁸, è stata confermata la linea avanzata nella proposta iniziale della Commissione di non imporre agli Stati membri la designazione delle autorità di protezione di dati quali autorità competenti rispetto all'applicazione generale dell'*AI Act*. Invece, la competenza in materia di vigilanza sull'applicazione del regolamento sull'IA spetterà, come regola generale, alle autorità di controllo da esso istituite o designate appositamente e soltanto in via d'eccezione alle altre autorità nazionali.

La potenziale attribuzione del potere di vigilanza a diverse autorità comporterà la ricerca di uno stringente coordinamento tra queste al fine di garantire l'effettiva ed efficace applicazione del regolamento sul piano nazionale. La portata dell'interazione tra autorità di controllo afferenti a distinti ambiti di intervento è stata affrontata (per la prima volta) dalla Corte di giustizia nella recente pronuncia relativa al caso *Meta Platforms e a.*, del 4 luglio 2023²⁹. Nel caso di specie, si lamentava il fatto che l'interpretazione, da parte delle autorità antitrust,

regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework, in *AI & Soc*, 2021, p. 623 ss.; G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, p. 207 ss.; T. FROSINI, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, n. 1, 2022, p. 273 ss.

²⁸ EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), punto 47.

²⁹ In dottrina P. MANZINI, *Antitrust e privacy: la strana coppia*, in *Quaderni AISDUE*, n. 10, 2023, p. 196 ss.; I. GRAEF, *Meta platforms: How the CJEU leaves competition and data protection authorities with an assignment*, in *MJECL*, 2023, p. 325 ss.; P. G. PICHT, *CJEU on Facebook: GDPR Processing Justifications and Application Competence*, in *Gewerblicher Rechtsschutz und Urheberrecht*, n. 16, 2023, p. 1169 ss., M. PREVIADELLO, *L'obbligo di leale cooperazione tra autorità nazionali garanti della concorrenza e autorità di controllo istituite dal RGPD nella sentenza Meta Platforms e a.*, in *Quaderni AISDUE*, n. 1, 2024, p. 1 ss.

delle disposizioni del RGPD al fine di constatare una violazione del diritto della concorrenza avrebbe determinato un potenziale *vulnus* alle competenze delle autorità per la *privacy*. Ebbene, qui i giudici hanno riconosciuto alle autorità amministrative degli Stati membri la possibilità di esercitare una competenza condivisa, purché non sostitutiva³⁰, desumendo una serie di obblighi di collaborazione e di coordinamento tra dette autorità direttamente dal principio di leale collaborazione, previsto dall'art. 4, par. 3, TUE³¹. Pare pacifico sostenere che, se questo ragionamento vale per autorità di controllo con compiti e obiettivi distinti ma che ad un certo punto possono convergere, a maggior ragione le autorità amministrative espressamente titolate ad intervenire per vigilare sull'attuazione dell'*AI Act* dovranno cooperare tra loro al fine di garantire, da un lato, l'effettiva applicazione del diritto settoriale e, dall'altro, la coerenza del sistema di protezione istituito dal regolamento sull'IA³². Questa esigenza è pure desumibile dalla risalente giurisprudenza della Corte di giustizia, secondo cui le autorità amministrative degli Stati membri devono rispettarsi ed assistersi reciprocamente nell'adempimento dei compiti derivanti dai Trattati, adottare ogni misura necessaria per assicurare l'adempimento degli obblighi risultanti dagli atti adottati dalle istituzioni, nonché evitare di adottare qualsiasi misura che potrebbe compromettere il raggiungimento degli obiettivi dell'Unione³³. Ad ogni modo, dal momento che questo aspetto relativo alla cooperazione tra autorità nazionali non è disciplinato esaustivamente dall'*AI Act*, è probabile – oltre che auspicabile – che in futuro sia richiesto ai giudici di

³⁰ 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*, Torino, 2021, p. 422 ss.

³¹ *Meta Platforms e a.*, sopra citata, punto 53.

³² Sul principio di leale cooperazione tra gli Stati membri, si veda P. DE PASQUALE, *Commento all'art. 4 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, II ed., Milano, 2014, spec. p. 28 ss.; M. KLAMERT, *Article 4 TEU*, in M. KELLERBAUER ET AL. (eds.), *The EU Treaties and the Charter of Fundamental Rights — A Commentary*, Oxford, 2019, p. 35 ss.; F. CASOLARI, *La leale cooperazione tra Stati membri e Unione europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Napoli, 2020.

³³ Corte giust. 7 novembre 2013, C-518/11, *UPC Nederland*, punto 59; 1° agosto 2022, C-14/21 e C-15/21, *Sea Watch*, punto 156.

Lussemburgo di pronunciarsi in modo tale da escludere, o quantomeno mitigare, il rischio di divergenze tra le diverse autorità nazionali in merito al controllo sull'attuazione del regolamento.

4.2. Segue: a livello interstatale e sovranazionale

La regolamentazione introdotta dall'*AI Act* disciplina la cooperazione tra le autorità nazionali di controllo interessate a livello interstatale e la cooperazione di tali autorità con il Comitato europeo per l'intelligenza artificiale³⁴ e l'Ufficio per l'IA, incaricati di sorvegliare sulla corretta applicazione del regolamento nei vari Stati membri e di elaborare linee guida in materia, specialmente in relazione ai modelli fondativi e GPAI³⁵. In particolare, l'art. 74, par. 11, del regolamento prevede che le autorità di vigilanza del mercato degli Stati membri e la Commissione propongano attività congiunte al fine di promuovere la conformità, sensibilizzare e fornire orientamenti in relazione all'*AI Act* riguardo a specifiche categorie di sistemi di IA ad alto rischio che presentino un rischio grave in due o più Stati membri. Queste attività di natura congiunta dovrebbero basarsi sulla procedura prevista all'art. 9 del reg. 2019/1020 e sotto il coordinamento dell'Ufficio per l'IA³⁶.

Oltre che a raccordarsi sulle *best practices*, obiettivo questo dettato dall'impostazione generale dell'*AI Act* di prevenire più che reprimere eventuali pratiche, il regolamento prevede anche la possibilità di attivare indagini congiunte tra autorità di vigilanza. Ai sensi dell'art. 79,

³⁴ Come previsto dal considerando n. 149 dell'*AI Act*, al fine di facilitare l'attuazione agevole, efficace e armonizzata delle norme stabilite nell'*AI Act* viene istituito un Comitato europeo per l'intelligenza artificiale finalizzato a «riflettere i vari interessi dell'ecosistema dell'IA». A tal fine, ex art. 65, il Comitato sarà composto da un rappresentante per Stato membro, designato per tre anni e rinnovabile una sola volta. Per offrire una certa flessibilità agli Stati membri nella designazione dei loro rappresentanti all'interno del Comitato, che pur dovranno garantire obiettività e imparzialità, tali rappresentanti potranno appartenere a entità pubbliche dotate delle competenze e dei poteri pertinenti per facilitare il coordinamento e la coerenza a livello nazionale e contribuire all'adempimento dei compiti del comitato.

³⁵ Per approfondimenti, si rinvia al contributo di F. FERRI, *op. cit.*

³⁶ Peraltro, in riferimento alle presunte violazioni da parte di fornitori di GPAI, va detto che l'Ufficio per l'IA, pur esclusivamente competente, si attenderà una stretta collaborazione, in termini di segnalazioni e trasferimento di informazioni, da parte delle autorità di vigilanza nazionali.

par. 3, del regolamento, se l'autorità di vigilanza di uno Stato membro ritiene che la violazione non sia limitata al suo territorio nazionale ma possa avere un impatto transnazionale, dovrà informare la Commissione e gli altri Stati membri dei risultati della valutazione e delle azioni richieste al fornitore o all'utilizzatore del sistema di IA. In tali casi, dovrebbe dunque applicarsi *mutatis mutandis* la procedura relativa all'assistenza reciproca e allo scambio di informazioni nei casi transfrontalieri di cui alle disposizioni del capo VI del reg. 2019/1020. In aggiunta, l'*AI Act* prevede che qualsiasi autorità di vigilanza del mercato chieda assistenza all'Ufficio per l'IA qualora non sia in grado di concludere un'indagine su un sistema ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali su cui è costruito il sistema sottoposto ad indagine.

Degno di nota è, infine, l'art. 81 che conferma il ruolo predominante della Commissione all'interno del disegno complessivo del regolamento³⁷, attribuendole una serie di poteri che le permettono di prevalere sulle decisioni delle autorità nazionali. Infatti, è qui previsto che, qualora l'autorità di vigilanza del mercato di uno Stato membro sollevi obiezioni contro una misura adottata da un'altra autorità di vigilanza del mercato, o la Commissione ritenga che la misura sia contraria al diritto UE, quest'ultima consulterà l'autorità di vigilanza interessata e l'operatore, e valuterà se la misura nazionale è giustificata.

Questa impostazione riflette certamente l'esigenza di garantire che le autorità nazionali di vigilanza operino in modo coordinato, informato e congiunto nel momento in cui si ritenga che si possa verificare un utilizzo improprio dei sistemi di IA con impatto non solo a livello nazionale ma anche sovranazionale. Sebbene il sistema di vigilanza transnazionale figurato nell'*AI Act* appaia quindi apprezzabile grazie al rinvio a strumenti di mutua assistenza, esso è al contempo "zoppicante". In effetti, a parere di chi scrive, le disposizioni relative al sistema di vigilanza sono estremamente vaghe e, pur rinviando al più generale reg. 2019/1020, tradiscono un carattere più programmatico che precettivo. Questo approccio conferma il compromesso raggiunto nella costruzione di un meccanismo di vigilanza che, ben lungi dall'avere un carattere decisamente sovranazionale, si è assestato sulle esigenze

³⁷ Per approfondimenti, si rinvia al contributo di F. FERRI, *op. cit.*

nazionali di controllo. A conferma di ciò, occorre sottolineare il cambiamento che caratterizza la versione finale dell'*AI Act* rispetto alla proposta della Commissione. Infatti, il Comitato europeo per l'IA doveva essere composto dalle autorità nazionali di vigilanza, compreso evidentemente il Garante europeo: in altre parole, in quanto autorità di sintesi delle singole autorità di vigilanza, il Comitato si sarebbe auto promosso ad autorità indipendente europea. Tuttavia, questo impianto è stato mitigato a seguito dell'accordo raggiunto nel trilatero, attribuendo la funzione di *trait-d'union* rispetto alla cooperazione amministrativa al sottogruppo permanente per la vigilanza del mercato (ADCO) per l'*AI Act*³⁸, sotto il coordinamento della Commissione europea che mantiene ben saldo il potere regolatorio. Resta da chiedersi fino a che punto il Comitato, che potrà sostanzialmente adottare solo atti di *soft law*, potrà garantire una supervisione (seppur debole) sull'applicazione uniforme del regolamento. Ciò, tenuto poi conto che il Garante europeo parteciperà al Comitato solamente in qualità di osservatore, smorzando così il carattere sovranazionale del coordinamento.

A fronte di ciò, il rischio che le autorità degli Stati membri possano rivendicare la competenza, determinando una frammentazione dell'applicazione ed eventualmente l'adozione di decisioni contrastanti, non è trascurabile, specialmente per i destinatari di indagini e sanzioni amministrative. Sarà pertanto necessario che le manovre delle autorità si fondino, di nuovo, sul principio di leale collaborazione previsto dall'art. 4, par. 3, TUE, auspicabilmente attingendo ai requisiti e alle modalità di cooperazione tra autorità nazionali già individuati dalla Corte di giustizia nel noto caso *Facebook Ireland e a.*³⁹. In

³⁸ Ai sensi dell'art. 65, par. 6, dell'*AI Act*, il Comitato sarà composto da due sottogruppi permanenti per fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni relative. Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per l'*AI Act* ai sensi dell'art. del regolamento (UE) 2019/1020. In conformità poi dell'art. 33 di quest'ultimo regolamento, la Commissione dovrebbe sostenere le attività del sottogruppo permanente per la vigilanza del mercato effettuando valutazioni o studi di mercato, in particolare al fine di individuare quelli che richiedono un coordinamento specifico e urgente tra le autorità di vigilanza del mercato.

³⁹ Corte giust. 15 giugno 2021, C-645/19. Per commenti, si veda S. BRETTEAUER, *Extended powers for other supervisory authorities concerned in the case of cross-border data processing: Facebook Ireland*, in *CMLR*, n. 2, 2022, p. 1543 ss.; L.

quell'occasione, infatti, i giudici di Lussemburgo avevano confermato la ripartizione delle competenze tra le autorità di vigilanza di diversi Stati membri per preservare il cd. “*one-stop shop mechanism*”⁴⁰, sottolineando l'importanza di una cooperazione non solo efficace (come espressamente previsto dal RGPD) ma anche leale tra di loro. Ciò, per tornare al regolamento sull'IA, al fine di garantire un'attuazione coerente e omogenea della normativa oltretutto una maggiore prevedibilità per i soggetti coinvolti nella fornitura e nell'utilizzo di sistemi di IA⁴¹. Vista la portata dell'*AI Act* e l'impatto della sua applicazione, è certo che la Corte di giustizia sarà in futuro chiamata a pronunciarsi anche su questi aspetti.

5. Riflessioni conclusive

Il sistema di *governance* relativo alla vigilanza sull'applicazione dell'*AI Act* è particolarmente complesso, tentando di porsi come un correttivo di natura complementare e ancillare rispetto ai meccanismi di tutela *ex ante*. Non solo. Il sistema illustrato pare fortemente orientato a tutelare, tanto sul piano organizzativo quanto funzionale, le esigenze di controllo sull'IA degli Stati membri. Questo è confermato, in particolare, dal tenore delle disposizioni sulle autorità di vigilanza nazionali che garantiscono ampia discrezionalità agli Stati nella designazione di dette autorità.

Nel quadro normativo dell'Unione, questo secondo punto è particolarmente dirimente. Infatti, come si è avuto modo di sottolineare, sul piano costituzionale è certamente rilevante il rinvio ad uno dei principi cardine del diritto UE, ovvero il principio di leale cooperazione che, come noto, non si esaurisce nella reciproca assistenza per l'adempimento dei compiti derivanti dai trattati ma anche nell'astensione da qualsiasi misura che rischi di mettere in pericolo la

CHEMLALI, *The competence of non-lead supervisory authority under the EU GDPR 'S one-stop-shop mechanism: CJEU judgment in Facebook and Others (C-645/19)*, in *Journal of Media Law*, n. 2, 2022, p. 208 ss.

⁴⁰ Previsto dall'art. 60 del RGPD, tale meccanismo (denominato in italiano ‘sportello unico’) è stato poi incorporato e dettagliato nelle linee guida adottate il 28 marzo 2023 dal Garante europeo sull'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento.

⁴¹ *Facebook Ireland e a.*, sopra citata, punti 53, 60, 63 e 72.

realizzazione degli obiettivi dell'Unione. Richiedere, dunque, che le autorità di vigilanza si coordinino, sia sul piano interno che su quello sovranazionale, per garantire l'effettività del regolamento sull'IA rappresenta certamente un obbligo di leale cooperazione a cui pure le autorità amministrative devono conformarsi nel caso di specie. Al contempo, però, non può sfuggire l'assenza di soggetto indipendente che garantisca un coordinamento effettivo e stringente tra le autorità di vigilanza, compreso il Garante europeo per quanto attiene le istituzioni dell'Unione. Infatti, per come configurato nell'*AI Act*, il sottogruppo per la vigilanza del mercato del Comitato europeo per l'IA rappresenta una semplice piattaforma di cooperazione e scambio tra le autorità nazionali senza determinanti poteri di armonizzazione. In assenza di un sistema di raccordo indipendente a livello sovranazionale, sarà la Commissione europea, e dunque un'istituzione politica nonché l'esecutivo dell'Unione, ad assumere il ruolo di “super controllore” del sistema di vigilanza, potendo valutare, in caso di dubbi, se le misure adottate dalle autorità nazionali rispetto ai sistemi di IA immessi nel mercato siano giustificate.

In conclusione, per come attualmente configurata, nonostante la rilevanza delle misure sanzionatorie e la possibilità per le autorità di richiedere il ritiro dal mercato o il richiamo dei prodotti, la disciplina complessiva in materia di vigilanza non appare del tutto sufficiente a garantire un'applicazione efficace. L'esperienza del RGPD mostra che un eccessivo affidamento sull'*enforcement* delle autorità nazionali espone al rischio di difformità applicative, a causa delle notevoli divergenze di risorse e prassi di intervento nei diversi Stati membri⁴². Com'è usuale in campo tecnologico, poi, si pone il problema di possibili difformità nei criteri di valutazione degli *standard* tecnici, che sarà tanto più pregnante in un settore, quello dell'IA, caratterizzato da un elevato numero di attori e di *standard* diversi. Il successo dell'*AI Act* si misurerà, dunque, anche sulla capacità di vigilanza da parte delle autorità ma anche in quella delle istituzioni dell'Unione – *in primis* Commissione europea e Corte di giustizia – di lavorare per individuare dei profili di cooperazione stringente tra le singole autorità di controllo,

⁴² G. DE MINICO, *Autorità indipendenti e algoritmi: una famiglia disfunzionale*, in *Osservatorio sulle fonti*, n. 2, 2021, p. 981 ss.

permettendo a queste di stare al passo con lo sviluppo estremamente celere dei sistemi di IA.

ABSTRACT (ITA)

Il complessivo sistema di vigilanza previsto dal regolamento sull'intelligenza artificiale si articola su un doppio livello, quello sovranazionale e quello nazionale, ed è finalizzato a completare il meccanismo di controllo e verifica precedente all'immissione nel mercato dei sistemi di intelligenza artificiale. Nello specifico, il regolamento prevede che gli Stati membri designino una o più autorità nazionali competenti, con funzioni di vigilanza del mercato e della sua corretta applicazione, con possibilità di esercitare poteri sanzionatori. D'altro canto, il Garante europeo per la protezione dei dati è stato designato quale autorità di vigilanza del mercato competente per i sistemi di IA utilizzati da istituzioni, organi e organismi dell'Unione. Questa impostazione di *governance*, frammentata e foriera di tensioni, richiederà un importante sforzo di coordinamento, sia sul piano interno che su quello sovranazionale, quale espressione del principio di leale cooperazione previsto dall'art. 4, par. 3, TUE e ribadito a più riprese dalla recente giurisprudenza della Corte di giustizia in materia di vigilanza.

ABSTRACT (ENG)

The overall supervisory system provided for by the Regulation on Artificial Intelligence is divided into two levels, supranational and national, and is aimed at completing the control and verification mechanism prior to the placing of artificial intelligence systems on the market. Specifically, the Regulation provides that Member States shall designate one or more competent national authorities, with functions of market surveillance and its proper application, with the possibility of exercising sanctioning powers. On the other hand, the European Data Protection Supervisor has been designated as the competent market surveillance authority for AI systems used by Union institutions, bodies, offices and agencies. This approach to *governance*, which is fragmented and fraught with tensions, will require a major effort of coordination, both internally and supranationally, as an expression of the principle of sincere cooperation provided for in Art. 4(3) TEU and reaffirmed on several occasions by the recent case-law of the Court of Justice.