Parlamento europeo e Consiglio dell'Unione europea - Regolamento (UE) del 13 giugno 2024 n. 2024/1689
Pubblicato sulla "Gazzetta Ue" del 12 luglio 2024
come modificato dal Regolamento (UE) dell'8 luglio 2026 n. 2026/1744
Pubblicato sulla "Gazzetta Ue" del 24 luglio 2026

Digital Omnibus AI: i sistemi ad alto rischio con obblighi di attuazione più lenti per i produttori

Sono trascorsi appena due anni tra il varo del cosiddetto "IA Act" e il cosiddetto «Omnibus digitale sull'IA» dell'8 luglio 2026, pubblicato nella Gazzetta ufficiale dell'Unione europea il 24 luglio 2026, e già la disciplina dell'intelligenza artificiale cambia assetto. Il regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio dell'8 luglio 2026, noto appunto come «Omnibus digitale sull'IA», modifica infatti il regolamento (UE) 2024/1689 e i regolamenti (UE) 2018/1139 e (UE) 2023/1230, introducendo un significativo intervento di semplificazione delle norme che disciplinano gli algoritmi. Nel testo pubblicato in queste pagine ripercorriamo tutte le modifiche apportate dal regolamento (UE) 2026/1744 al regolamento (UE) 2024/1689, evidenziando in nero le disposizioni novellate.

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 (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

CAPO I (*)
DISPOSIZIONI GENERALI

ARTICOLO 1
Oggetto

1. Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione.

2. Il presente regolamento stabilisce:

a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione;

b) divieti di talune pratiche di IA;

c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi;

d) regole di trasparenza armonizzate per determinati sistemi di IA;

e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali;

f) regole in materia di monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione;

g) misure a sostegno dell'innovazione, con particolare attenzione alle piccole imprese a media capitalizzazione e alle piccole e medie imprese (PMI), comprese le start-up.

ARTICOLO 2
Ambito di applicazione

1. Il presente regolamento si applica:

(*) Le parti evidenziate in nero sono quelle modificate dal Regolamento (UE) n. 2026/1744.

a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;

b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione;

c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione;

d) agli importatori e ai distributori di sistemi di IA;

e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio;

f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione;

g) alle persone interessate che si trovano nell'Unione.

2. Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, si applicano unicamente l'articolo 6, paragrafo 1, l'articolo 60 bis e gli articoli da 102 a 112. Gli articoli 57, 58 e 59 si applicano solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati in tale normativa di armonizzazione dell'Unione.

3. Il presente regolamento non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze.

Il presente regolamento non si applica ai sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

4. Il presente regolamento non si applica alle autorità pubbliche di un paese terzo né alle organizzazioni internazionali che rientrano nell'ambito di applicazione del presente regolamento a norma del paragrafo 1, laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri, a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone.

5. Il presente regolamento non pregiudica l'applicazione delle disposizioni sulla responsabilità dei prestatori di servizi intermediari di cui al capo II del regolamento (UE) 2022/2065.

6. Il presente regolamento non si applica ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici.

7. Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi gli articoli 4 bis e 59 del presente regolamento.

8. Il presente regolamento non si applica alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio. Tali attività sono svolte in conformità del diritto dell'Unione applicabile. Le prove in condizioni reali non rientrano in tale esclusione.

9. Il presente regolamento lascia impregiudicate le norme stabilite da altri atti giuridici dell'Unione in materia di protezione dei consumatori e di sicurezza dei prodotti.

10. Il presente regolamento non si applica agli obblighi dei deployer che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale.

11. Il presente regolamento non osta a che l'Unione o gli Stati membri mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contratti collettivi più favorevoli ai lavoratori.

12. Il presente regolamento non si applica ai sistemi di IA rilasciati con licenza libera e open source, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o come sistema di IA rientrante nell'ambito di applicazione dell'articolo 5 o 50.

13. Per i sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 1, l'applicazione dei requisiti o degli obblighi specifici di cui agli articoli da 9 a 15 e da 17 a 25 può essere limitata se e nella misura in cui:

a) la normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, stabilisce requisiti o obblighi che garantiscono un livello equivalente o superiore di protezione della salute, della sicurezza o dei diritti fondamentali a quello del requisito o dell'obbligo in questione; e

b) tale limitazione non riduce il livello complessivo di protezione previsto dal presente regolamento.

Entro il 2 agosto 2027 la Commissione adotta atti delegati conformemente all'articolo 97 al fine di integrare il presente regolamento specificando i sistemi di IA ad alto rischio interessati, i requisiti o gli obblighi che possono essere limitati, le condizioni alle quali si applica tale limitazione e la portata della stessa.

ARTICOLO 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

2) «rischio»: la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso;

3) «fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;

4) «deployer»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;

5) «rappresentante autorizzato»: una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento;

6) «importatore»: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;

7) «distributore»: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione;

8) «operatore»: un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore;

9) «immissione sul mercato»: la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione;

10) «messa a disposizione sul mercato»: la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito;

11) «messa in servizio»: la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista;

12) «finalità prevista»: l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;

13) «uso improprio ragionevolmente prevedibile»: l'uso di un sistema di IA in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi, ivi compresi altri sistemi di IA, ragionevolmente prevedibile;

14) «componente di sicurezza»: un componente di un prodotto o di un sistema di IA che svolge una funzione di sicurezza per tale prodotto o sistema di IA o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni; ai fini della presente definizione, un componente svolge una funzione di sicurezza se la sua finalità prevista è prevenire o attenuare i rischi per la salute e la sicurezza di persone o beni;

14-bis) «microimprese, piccole e medie imprese» o «PMI»: microimprese, piccole o medie imprese quali definite all'articolo 2 dell'allegato della raccomandazione 2003/361/CE;

14-ter) «piccole imprese a media capitalizzazione»: piccole imprese a media capitalizzazione quali definite al punto 2 dell'allegato della raccomandazione (UE) 2025/1099;

15) «istruzioni per l'uso»: le informazioni comunicate dal fornitore per informare il deployer in particolare della finalità prevista e dell'uso corretto di un sistema di IA;

16) «richiamo di un sistema di IA»: qualsiasi misura volta a ottenere la restituzione al fornitore, la messa fuori servizio o la disabilitazione dell'uso di un sistema di IA messo a disposizione dei deployer;

17) «ritiro di un sistema di IA»: qualsiasi misura volta a impedire che un sistema di IA nella catena di approvvigionamento sia messo a disposizione sul mercato;

18) «prestazioni di un sistema di IA»: la capacità di un sistema di IA di conseguire la finalità prevista;

19) «autorità di notifica»: l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio;

20) «valutazione della conformità»: la procedura atta a dimostrare se i requisiti di cui al capo III, sezione 2, relativi a un sistema di IA ad alto rischio sono stati soddisfatti;

21) «organismo di valutazione della conformità»: un organismo che svolge per conto di terzi attività di valutazione della conformità, incluse prove, certificazioni e ispezioni;

22) «organismo notificato»: un organismo di valutazione della conformità notificato in conformità del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;

23) «modifica sostanziale»: una modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che non è prevista o programmata nella valutazione iniziale della conformità effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo III, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato;

24) «marcatura CE»: una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al capo III, sezione 2, e in altre normative di armonizzazione dell'Unione applicabili e che ne prevedono l'apposizione;

25) «sistema di monitoraggio successivo all'immissione sul mercato»: tutte le attività svolte dai fornitori di sistemi di IA al fine diraccogliere e analizzare l'esperienza maturata tramite l'uso dei sistemi di IA che immettono sul mercato o che mettono in servizio, al fine di individuare eventuali necessità di immediate azioni correttive o preventive;

26) «autorità di vigilanza del mercato»: l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020;

27) «norma armonizzata»: la norma armonizzata di cui all'articolo 2, punto 1), lettera c), del regolamento (UE) n. 1025/2012;

28) «specifiche comuni»: un insieme di specifiche tecniche quali definite all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012, che forniscono i mezzi persoddisfare determinati requisitistabiliti a norma del presente regolamento;

29) «dati di addestramento»: i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;

30) «dati di convalida»: i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (underfitting) o l'eccessivo (overfitting) adattamento ai dati di addestramento;

31) «set di dati di convalida»: un set di dati distinto o costituito da una partizione fissa o variabile del set di dati di addestramento;

32) «dati di prova»: i dati utilizzati per fornire una valutazione indipendente delsistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

33) «dati di input»: i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output;

34) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica,quali le immagini facciali o i dati dattiloscopici;

35) «identificazione biometrica»: il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati;

36) «verifica biometrica»: la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza;

37) «categorie particolari di dati personali»: le categorie di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725;

38) «dati operativi sensibili»: dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali;

39) «sistema di riconoscimento delle emozioni»: un sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

40) «sistema di categorizzazione biometrica»: un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive;

41) «sistema di identificazione biometrica remota»: un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento;

42) «sistema di identificazione biometrica remota in tempo reale»: un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione;

43) «sistema di identificazione biometrica remota a posteriori»: un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota «in tempo reale»;

44) «spazio accessibile al pubblico»: qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità;

45) «autorità di contrasto»:

a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure

b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

46) «attività di contrasto»: le attività svolte dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;

47) «ufficio per l'IA»: la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gen-

naio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione;

48) «autorità nazionale competente»: un'autorità di notifica o un'autorità di vigilanza del mercato; per quanto riguarda i sistemi di IA messi in servizio o utilizzati da istituzioni, organi e organismi dell'Unione, i riferimenti alle autorità nazionali competenti o alle autorità di vigilanza del mercato contenuti nel presente regolamento si intendono fatti al Garante europeo della protezione dei dati;

49) «incidente grave»: un incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, causa una delle conseguenze seguenti:

a) il decesso di una persona o gravi danni alla salute di una persona;

b) una perturbazione grave e irreversibile della gestione o del funzionamento delle infrastrutture critiche;

c) la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali;

d) gravi danni alle cose o all'ambiente;

50) «dati personali»: i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

51) «dati non personali»: dati diversi dai dati personali di cui all'articolo 4, punto 1), del regolamento (UE) 2016/679;

52) «profilazione»: la profilazione quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679;

53) «piano di prova in condizioni reali»: un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali;

54) «piano dello spazio di sperimentazione»: un documento concordato tra il fornitore partecipante e l'autorità competente in cui sono descritti gli obiettivi, le condizioni, il calendario, la metodologia e i requisiti relativamente alle attività svolte all'interno dello spazio di sperimentazione;

55) «spazio di sperimentazione normativa per l'IA»: un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare;

56) «alfabetizzazione in materia di IA»: le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare;

57) «prova in condizioni reali»: la prova temporanea di un sistema di IA per la sua finalità prevista in condizioni reali al di fuori di un laboratorio o di un ambiente altrimenti simulato al fine di raccogliere dati affidabili e solidi e di valutare e verificare la conformità del sistema di IA ai requisiti del presente regolamento e che non è considerata immissione sul mercato o messa in servizio del sistema di IA ai sensi del presente regolamento, purché siano soddisfatte tutte le condizioni di cui all'articolo 57 o 60;

58) «soggetto»: ai fini della prova in condizioni reali, una persona fisica che partecipa a prove in condizioni reali;

59) «consenso informato»: l'espressione libera, specifica, inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare;

60) «deep fake»: un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona;

61) «infrazione diffusa»: qualsiasi azione od omissione contraria al diritto dell'Unione che tutela gli interessi delle persone:

a) che abbia arrecato o possa arrecare un danno agli interessi collettivi di persone che risiedono in almeno due Stati membri diversi dallo Stato membro in cui:

i) ha avuto origine o si è verificato l'azione o l'omissione in questione;

ii) è ubicato o stabilito il fornitore interessato o, se del caso, il suo rappresentante autorizzato; oppure

iii) è stabilito il deployer, quando la violazione è commessa dal deployer;

b) che abbia arrecato, arrechi o possa arrecare un danno agli interessi collettivi di persone e che presenti caratteristiche comuni, compresa la stessa pratica illecita e lo stesso interesse leso e che si verifichi simultaneamente, commessa dal medesimo operatore, in almeno tre Stati membri;

62) «infrastruttura critica»: infrastruttura critica quale definita all'articolo 2, punto 4), della direttiva (UE) 2022/2557;

63) «modello di IA per finalità generali»: un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;

64) «capacità di impatto elevato»: capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati;

65) «rischio sistemico»: un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società

nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore;

66) «sistema di IA per finalità generali»: un sistema di IA basato su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA;

67) «operazione in virgola mobile»: qualsiasi operazione o assegnazione matematica che comporta numeri in virgola mobile, un sottoinsieme dei numeri reali generalmente rappresentati sui computer mediante un numero intero con precisione fissa avente come fattore di scala un esponente intero di una base fissa;

68) «fornitore a valle»: un fornitore di un sistema di IA, compreso un sistema di IA per finalità generali, che integra un modello di IA, indipendentemente dal fatto che il modello di IA sia fornito dallo stesso e integrato verticalmente o fornito da un'altra entità sulla base di relazioni contrattuali.

Articolo 4
Alfabetizzazione in materia di IA

1. I fornitori e i deployer di sistemi di IA adottano misure volte a sostenere lo sviluppo dell'alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati. Tale obbligo non impone ai fornitori o ai deployer di garantire un livello specifico di alfabetizzazione in materia di IA per alcuna persona.

2. La Commissione e gli Stati membri sostengono e agevolano gli sforzi dei fornitori e dei deployer di sistemi di IA, in particolare delle PMI, nell'adempimento dell'obbligo di cui al paragrafo 1 del presente articolo. A tal fine, la Commissione pubblica esempi pratici di come adempiere a tale obbligo sulla piattaforma unica di informazione di cui all'articolo 62, paragrafo 3, lettera b).

3. Il consiglio per l'IA adotta raccomandazioni, tenendo conto dei quadri europei delle competenze, per sostenere la Commissione e gli Stati membri nella promozione dell'alfabetizzazione in materia di IA richiesta a norma del paragrafo 1, anche stabilendo obiettivi comuni.

Articolo 4-bis
Trattamento di categorie particolari di dati personali ai fini del rilevamento e della correzione delle distorsioni

1. Nella misura strettamente necessaria a garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio in conformità dell'articolo 10, paragrafo 2, lettere f) e g), del presente regolamento, i fornitori di tali sistemi possono eccezionalmente trattare categorie particolari di dati personali, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche. Oltre alle disposizioni di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680, a seconda dei casi, sono soddisfatte, affinché tale trattamento avvenga, tutte le condizioni seguenti:

a) il rilevamento e la correzione delle distorsioni non possono essere realizzati efficacemente mediante il trattamento di altri dati, compresi i dati sintetici o anonimizzati;

b) le categorie particolari di dati personali sono soggette a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione;

c) le categorie particolari di dati personali sono soggette a misure tese a garantire che i dati personali trattati siano resi sicuri e protetti nonché soggetti a garanzie adeguate, ivi compresi controlli e documentazione rigorosi dell'accesso, al fine di evitare abusi e garantire che solo le persone autorizzate e sottostanti a opportuni obblighi di riservatezza abbiano accesso a tali dati personali;

d) le categorie particolari di dati personali non sono trasmesse, trasferite o altrimenti consultate da terzi;

e) le categorie particolari di dati personali vengono cancellate dopo che la distorsione è stata corretta oppure i dati personali hanno raggiunto la fine del loro periodo di conservazione, a seconda di quale delle due condizioni si verifica per prima; e

f) i registri delle attività di trattamento a norma dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 comprendono i motivi per cui il trattamento delle categorie particolari di dati personali era strettamente necessario per rilevare e correggere distorsioni e i motivi per cui tale obiettivo non poteva essere raggiunto mediante il trattamento di altri dati.

2. I fornitori e i deployer di altri sistemi e modelli di IA e i deployer di sistemi di IA ad alto rischio possono eccezionalmente trattare categorie particolari di dati personali nella misura in cui:

a) tale trattamento è strettamente necessario per garantire il rilevamento e la correzione di possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future; e

b) sono applicate tutte le condizioni e le garanzie di cui al paragrafo 1.

Il presente paragrafo non crea alcun obbligo di rilevare e correggere tali distorsioni.

Capo II
PRATICHE DI IA VIETATE

Articolo 5
Pratiche di IA vietate

1. Sono vietate le pratiche di IA seguenti:

a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingan-

nevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;

b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo;

b-bis) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che genera o manipola immagini, video e audio realistici o materiale analogo delle parti intime di una persona fisica riconoscibile, o di una persona fisica riconoscibile che partecipi ad atti sessualmente espliciti senza il consenso liberamente prestato, specifico, informato e inequivocabile di tale persona per tale generazione o manipolazione;

b-ter) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che genera o manipola materiale o spettacoli ai sensi dell'articolo 2, lettere c) ed e), della direttiva 2011/93/UE, salvo nei casi in cui sussista una causa di giustificazione ai sensi del diritto nazionale;

c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IAper la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;

d) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa;

e) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;

f) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza;

g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto;

h) l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrastoa meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

i) la ricerca mirata di specifichevittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

iii) lalocalizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

La lettera h) del primo comma lascia impregiudicato l'articolo 9 del regolamento (UE) 2016/679 per quanto riguarda il trattamento dei dati biometrici a fini diversi dall'attività di contrasto.

1-bis. Ai fini del paragrafo 1, primo comma, lettere b-bis) e b-ter):

a) l'immissione sul mercato o la messa in servizio di un sistema di IA che genera o manipola materiale o spettacoli di cui al paragrafo 1, primo comma, lettere b-bis) o b-ter), è vietata solo se:

i) la generazione o la manipolazione costituiscono la finalità prevista del sistema di IA; oppure

ii) la progettazione, l'addestramento, l'architettura, le capacità o le funzionalità del sistema con le quali l'utente interagisce direttamente (user-facing), rendono tale generazione o manipolazione un risultato ragionevolmente prevedibile e riproducibile, senza richiedere modifiche tecniche significative, e il sistema

non dispone di misure tecniche di sicurezza ragionevoli e adeguate e di altre garanzie per prevenire in modo affidabile tale generazione o manipolazione, tenendo conto di un uso improprio ragionevolmente prevedibile, e per correggere gli usi impropri osservati o segnalati;

b) l'uso di un sistema di IA che genera o manipola il materiale o gli spettacoli di cui al paragrafo 1, primo comma, lettere b-bis) e b-ter), è vietato solo se il deployer utilizza il sistema al fine di generare o manipolare tale materiale o tali spettacoli.

1 ter. Ai fini del paragrafo 1, primo comma, lettera b-bis), non costituisce manipolazione un sistema di IA che manipola il materiale in un modo che non aumenta l'esposizione di parti intime ritratte né altera la natura di eventuali atti sessualmente espliciti ritratti.

2. L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), è applicato ai fini di cui a tale lettera, solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:

a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema;

b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

L'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. L'uso del sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo.

3. Ai fini del paragrafo 1, primo comma, lettera h), e del paragrafo 2, ogniuso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria oda un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al paragrafo 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati.

L'autorità giudiziaria competente o un'autorità amministrativa indipendente la cui decisione è vincolante rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota «in tempo reale» in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, primo comma, lettera h), come indicato nella richiesta e, in particolare, rimane limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale. Nel decidere in merito alla richiesta, tale autorità tiene conto degli elementi di cui al paragrafo 2. Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota «in tempo reale».

4. Fatto salvo il paragrafo 3, ogni uso di un sistema di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto è notificato alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati conformemente alle regole nazionali di cui al paragrafo 5. La notifica contiene almeno le informazioni di cui al paragrafo 6 e non include dati operativi sensibili.

5. Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota.

6. Le autorità nazionali di vigilanza del mercato e le autorità nazionali per la protezione dei dati degli Stati membri cui è stato notificato l'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto a norma del paragrafo 4, presentano alla Commissione relazioni annuali su tale uso. A tal fine, la Commissione fornisce agli Stati membri e alle autori-

tà nazionali di vigilanza del mercato e di protezione dei dati un modello comprendente informazioni sul numero di decisioni che le autorità giudiziarie competenti, o un'autorità amministrativa indipendente la cui decisione è vincolante, hanno adottato in risposta alle richieste di autorizzazione a norma del paragrafo 3 e il loro esito.

7. La Commissione pubblica relazioni annuali sull'uso di sistemi di identificazione biometrica remota «in tempo reale» in spazi accessibili al pubblico a fini di attività di contrasto, fondate sui dati aggregati negli Stati membri sulla base delle relazioni annuali di cui al paragrafo 6. Tali relazioni annuali non includono dati operativi sensibili delle relative attività di contrasto.

8. Il presente articolo lascia impregiudicati i divieti che si applicano qualora una pratica di IA violi altre disposizioni di diritto dell'Unione.

CAPO III
SISTEMI DI IA AD ALTO RISCHIO

SEZIONE 1
Classificazione dei sistemi di IA come «ad alto rischio»

ARTICOLO 6
Regole di classificazione per i sistemi di IA ad alto rischio

1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.

1-bis. Ai fini del presente regolamento, compreso il paragrafo 1 del presente articolo, i sistemi di IA utilizzati esclusivamente per aspetti non legati alla sicurezza come assistenza agli utenti, ottimizzazione delle prestazioni, efficienza dei servizi, automazione o praticità o controllo della qualità non sono considerati componenti di sicurezza.

1-ter. In deroga al paragrafo 1 bis, i sistemi di IA il cui guasto o malfunzionamento metterebbe a rischio la salute e la sicurezza sono considerati componenti di sicurezza.

1-quater. Un prodotto che deve essere sottoposto a una valutazione della conformità da parte di terzi esclusivamente a causa di rischi diversi da quelli per la salute e la sicurezza, in particolare i rischi relativi alla distribuzione dello spettro radio o alle interferenze elettromagnetiche che non incidono sulla salute e sulla sicurezza, non è considerato conforme alla condizione di cui al paragrafo 1, lettera b).

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.

3. In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.

Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:

a) il sistema di IA è destinato a eseguire un compito procedurale limitato;

b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;

c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o

d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

4. Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione.

5. Dopo aver consultato il consiglio europeo per l'intelligenza artificiale («consiglio per l'IA»), ed entro il 2 febbraio 2026, la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio.

6. Alla Commissione è conferito il potere di adottare atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo aggiungendo nuove condizioni a quelle ivi stabilite, oppure modificandole, qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA che rientrano nell'ambito di applicazione dell'allegato III ma non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

7. La Commissione adotta atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo sopprimendo qualsiasi condizione ivi stabilita, qualora vi siano prove concrete e affidabili che è necessario al fine di mantenere il livello di protezione della salute, della sicurezza e dei diritti fondamentali previsto dal presente regolamento.

8. Eventuali modifiche alle condizioni di cui al paragrafo 3, secondo comma, adottate in conformità dei paragrafi 6 e 7 del presente articolo non riducono il livello globale di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione previsto dal presente regolamento e garantiscono la coerenza con gli atti delegati adottati a norma dell'articolo 7, paragrafo 1, e tengono conto degli sviluppi tecnologici e del mercato.

ARTICOLO 7

Modifiche dell'allegato III

omissis

SEZIONE 2

Requisiti per i sistemi di IA ad alto rischio

ARTICOLO 8

Conformità ai requisiti

omissis

ARTICOLO 9

Sistema di gestione dei rischi

omissis

ARTICOLO 10

Dati e governance dei dati

1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui al presente articolo, paragrafi 2, 3 e 4, e all'articolo 4 bis, paragrafo 1, ogniqualvolta siano utilizzati tali set di dati.

2. I set di dati di addestramento, convalida e prova sono soggetti a pratiche di governance e gestione dei dati adeguate alla finalità prevista del sistema di IA ad alto rischio. Tali pratiche riguardano in particolare:

a) le scelte progettuali pertinenti;

b) i processi di raccolta dei dati e l'origine dei dati, nonché la finalità originaria della raccolta nel caso di dati personali;

c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione;

d) la formulazione di ipotesi, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;

e) una valutazione della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;

f) un esame atto a valutare le possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future;

g) le misure adeguate per individuare, prevenire e attenuare le possibili distorsioni individuate conformemente alla lettera f);

h) l'individuazione di lacune o carenze pertinenti nei dati tali da pregiudicare il rispetto del presente regolamento e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o a livello di una combinazione degli stessi.

4. I set di dati tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico ambito geografico, contestuale, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

5. Soppresso

6. Per lo sviluppo di sistemi di IA ad alto rischio che non utilizzano tecniche che prevedono l'addestramento di modelli di IA, i paragrafi 2, 3 e 4 del presente articolo e l'articolo 4-bis, paragrafo 1, si applicano solo ai set di dati di prova.

ARTICOLO 11

Documentazione tecnica

1. La documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio di tale sistema ed è tenuta aggiornata.

Tale documentazione tecnica è redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui alla presente sezione e da fornire alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV. Le PMI, comprese le start-up, e le piccole imprese a media capitalizzazione possono fornire in modo semplificato gli elementi della documentazione tecnica specificati nell'allegato IV. A tal fine la Commissione definisce un modulo di documentazione tecnica semplificata che risponda alle esigenze delle PMI, comprese le start-up, e delle piccole imprese a media capitalizzazione. Qualora decida di fornire in modo semplificato le informazioni richieste nell'allegato IV, una PMI, compresa una start-up, o una piccola impresa a media capitalizzazione, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano il modulo ai fini della valutazione della conformità.

2. Se è immesso sul mercato o messo in servizio un sistema di IA ad alto rischio connesso a un prodotto contemplato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, si redige un'unica documentazione tecnica contenente tutte le informazioni di cui al paragrafo 1 e le informazioni necessarie a norma di tali atti giuridici.

3. Alla Commissione è conferito il potere di adottare

atti delegati conformemente all'articolo 97 al fine di modificare l'allegato IV ove necessario per garantire che, alla luce del progresso tecnico, la documentazione tecnica fornisca tutte le informazioni necessarie per valutare la conformità del sistema ai requisiti di cui alla presente sezione.

ARTICOLO 12
Conservazione delle registrazioni
omissis

ARTICOLO 13
Trasparenza e fornitura di informazioni ai deployer
omissis

ARTICOLO 14
Sorveglianza umana
omissis

ARTICOLO 15
Accuratezza, robustezza e cibersicurezza
omissis

SEZIONE 3
Obblighi dei fornitori e dei deployer dei sistemi di IA ad alto rischio e di altre parti

ARTICOLO 16
Obblighi dei fornitori dei sistemi di IA ad alto rischio
omissis

ARTICOLO 17
Sistema di gestione della qualità

1. I fornitori di sistemi di IA ad alto rischio istituiscono un sistema di gestione della qualità che garantisce la conformità al presente regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno gli aspetti seguenti:

a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio;

b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio;

c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio;

d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate;

e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti;

f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio;

g) il sistema di gestione dei rischi di cui all'articolo 9;

h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 72;

i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73;

j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle che forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate;

k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti;

l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento;

m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo.

2. L'attuazione degli aspetti di cui al paragrafo 1 è proporzionata alle dimensioni dell'organizzazione del fornitore, in particolare se questo è una PMI, anche nel caso di una start-up, o una piccola impresa a media capitalizzazione. I fornitori rispettano, in ogni caso, il grado di rigore e il livello di protezione necessari per garantire la conformità dei loro sistemi di IA ad alto rischio al presente regolamento.

3. I fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità o a una funzione equivalente a norma del pertinente diritto settoriale dell'Unione possono includere gli aspetti elencati al paragrafo 1 nell'ambito dei sistemi di gestione della qualità stabiliti a norma di tale diritto.

4. Per i fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità, ad eccezione del paragrafo 1, lettere g), h) e i), del presente articolo, si considera soddisfatto se sono soddisfatte le regole sui dispositivi o i processi di governance interna a norma del pertinente diritto dell'Unione in materia di servizi finanziari. A tal fine, si tiene conto delle norme armonizzate di cui all'articolo 40.

ARTICOLO 18
Conservazione dei documenti
omissis

ARTICOLO 19
Log generati automaticamente
omissis

ARTICOLO 20

Misure correttive e dovere di informazione

omissis

ARTICOLO 21

Cooperazione con le autorità competenti

omissis

ARTICOLO 22

Rappresentanti autorizzati dei fornitori dei sistemi di IA ad alto rischio

omissis

ARTICOLO 23

Obblighi degli importatori

omissis

ARTICOLO 24

Obblighi dei distributori

omissis

ARTICOLO 25

Responsabilità lungo la catena del valore dell'IA

1. Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:

a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;

b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;

c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.

2. Qualora si verifichino le circostanze di cui al paragrafo 1, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non è più considerato fornitore di quel determinato sistema di IA ai fini del presente regolamento.

Tale fornitore iniziale coopera strettamente con i nuovi fornitori e mette a disposizione le informazioni necessarie nonché fornisce l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio.

In particolare, l'obbligo di cui al secondo comma comprende, ove pertinente ai fini ivi specificati, quanto segue:

a) la messa a disposizione di documentazione tecnica sufficiente a valutare la conformità alle prescrizioni di cui all'articolo 16;

b) la comunicazione ai nuovi fornitori delle limitazioni note e delle modalità di guasto; e

c) la concessione ai nuovi fornitori di un accesso tecnico mirato, anche a fini di sperimentazione e convalida.

Il presente paragrafo non si applica nei casi in cui il fornitore iniziale abbia chiaramente specificato che il suo sistema di IA non deve essere trasformato in un sistema di IA ad alto rischio e pertanto non sia soggetto all'obbligo di cooperare con i nuovi fornitori e di consegnare la documentazione.

3. Nel caso dei sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fabbricante del prodotto è considerato il fornitore del sistema di IA ad alto rischio ed è soggetto agli obblighi di cui all'articolo 16, in una delle circostanze seguenti:

a) se il sistema di IA ad alto rischio è immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto;

b) se il sistema di IA ad alto rischio è messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato.

4. Il fornitore di un sistema di IA ad alto rischio e il terzo che fornisce un sistema di IA, un modello di IA, strumenti, servizi, componenti o processi utilizzati o integrati in un sistema di IA ad alto rischio precisano, mediante accordo scritto, le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari, sulla base dello stato dell'arte generalmente riconosciuto per permettere al fornitore del sistema di IA ad alto rischio di adempiere pienamente agli obblighi di cui al presente regolamento. Il presente paragrafo non si applica ai terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti, diversi dai modelli di IA per finalità generali, con licenza libera e open source.

L'ufficio per l'IA può elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio. Nell'elaborare tali clausole contrattuali tipo volontarie, l'ufficio per l'IA tiene conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali. Le clausole contrattuali tipo volontarie sono pubblicati e disponibili gratuitamente in un formato elettronico facilmente utilizzabile.

5. I paragrafi 2 e 3 lasciano impregiudicata la necessità di rispettare e proteggere i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali conformemente al diritto dell'Unione e nazionale.

ARTICOLO 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

omissis

ARTICOLO 27
Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

1. Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti:

a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;

b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;

c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;

d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;

e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;

f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.

2. L'obbligo di cui al paragrafo 1 si applica al primo uso del sistema di IA ad alto rischio. Il deployer può, in casi analoghi, basarsi su valutazioni d'impatto sui diritti fondamentali effettuate in precedenza o su valutazioni d'impatto esistenti effettuate da un fornitore. Se, durante l'uso del sistema di IA ad alto rischio, ritiene che uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il deployer adotta le misure necessarie per aggiornare le informazioni.

3. Una volta effettuata la valutazione di cui al paragrafo 1 del presente articolo, il deployer notifica all'autorità di vigilanza del mercato i suoi risultati, presentando il modello compilato di cui al paragrafo 5 del presente articolo nell'ambito della notifica. Nel caso di cui all'articolo 46, paragrafo 1, i deployer possono essere esentati da tale obbligo di notifica.

4. Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, nell'effettuare la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo, il deployer può includere rimandi alle sezioni pertinenti di tale valutazione d'impatto sulla protezione dei dati o includerne parti pertinenti nella valutazione d'impatto sui diritti fondamentali.

5. L'ufficio per l'IA elabora un modello di questionario, anche attraverso uno strumento automatizzato, per agevolare i deployer nell'adempimento dei loro obblighi a norma del presente articolo in modo semplificato. Tale modello dà ai deployer, se del caso, la possibilità di includere rimandi alle sezioni pertinenti della valutazione d'impatto sulla protezione dei dati o di includerne parti pertinenti nella valutazione d'impatto sui diritti fondamentali a norma del paragrafo 4.

SEZIONE 4
Autorità di notifica e organismi notificati

ARTICOLO 28
Autorità di notifica

1. Ciascuno Stato membro designa o istituisce almeno un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio. Tali procedure sono sviluppate nell'ambito della collaborazione tra le autorità di notifica di tutti gli Stati membri.

2. Gli Stati membri possono decidere che la valutazione e il monitoraggio di cui al paragrafo 1 siano eseguiti da un organismo nazionale di accreditamento ai sensi e in conformità del regolamento (CE) n. 765/2008.

3. Le autorità di notifica sono istituite, organizzate e gestite in modo tale che non sorgano conflitti di interesse con gli organismi di valutazione della conformità e che siano salvaguardate l'obiettività e l'imparzialità delle loro attività.

4. Le autorità di notifica sono organizzate in modo che le decisioni relative alla notifica di un organismo di valutazione della conformità siano prese da persone competenti, diverse da quelle che hanno effettuato la valutazione.

5. Le autorità di notifica non offrono né svolgono alcuna delle attività eseguite dagli organismi di valutazione della conformità, né servizi di consulenza su base commerciale o concorrenziale.

6. Le autorità di notifica salvaguardano la riservatezza delle informazioni che ottengono conformemente all'articolo 78.

7. Le autorità di notifica dispongono di un numero adeguato di dipendenti competenti per l'adeguata esecuzione dei relativi compiti. I dipendenti competenti dispongono, se del caso, delle competenze necessarie per svolgere le proprie funzioni in settori quali le tecnologie dell'informazione, l'IA e il diritto, compreso il controllo dei diritti fondamentali.

8. Le autorità di notifica designate ai sensi del presente regolamento responsabili dei sistemi di IA disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, garantiscono che l'organismo di valutazione della conformità che presenta domanda di designazione sia ai sensi del presente regolamento sia ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, abbia la possibilità di presentare un'unica domanda e di essere sottoposto a una procedura di

valutazione unificata per essere designato ai sensi del presente regolamento e della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora la pertinente normativa di armonizzazione dell'Unione preveda tale procedura di domanda unica e di valutazione unificata. A tal fine, le autorità di notifica designate ai sensi del presente regolamento e quelle designate ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, cooperano nelle loro valutazioni.

La procedura di domanda unica e di valutazione unificata di cui al presente paragrafo è messa a disposizione anche degli organismi notificati già designati ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, quando tali organismi notificati presentano domanda di designazione a norma del presente regolamento, a condizione che la pertinente normativa di armonizzazione dell'Unione preveda tale procedura.

Un organismo di valutazione della conformità designato ai sensi di più di un elemento della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, deve presentare una sola domanda per essere designato a norma del presente regolamento. Una designazione a norma del presente regolamento si applica a tutta la normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, per la quale è designato l'organismo di valutazione della conformità.

La procedura di domanda unica e di valutazione unificata evita inutili duplicazioni, è basata sulle procedure di designazione esistenti conformemente alla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, e garantisce la conformità ai requisiti relativi agli organismi notificati previsti sia conformemente al presente regolamento sia alla pertinente normativa di armonizzazione dell'Unione.

9. L'autorità di notifica designata ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, è anche l'autorità di notifica per la presentazione della domanda unica e per la procedura di valutazione unificata di cui al paragrafo 8, a meno che lo Stato membro non designi un'altra autorità di notifica ai fini del presente regolamento.

ARTICOLO 29

Domanda di notifica presentata dagli organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità presentano una domanda di notifica all'autorità di notifica dello Stato membro in cui sono stabiliti.

2. La domanda di notifica è accompagnata da una descrizione delle attività di valutazione della conformità, del modulo o dei moduli di valutazione della conformità e dei tipi di sistemi di IA per i quali tale organismo di valutazione della conformità dichiara di essere competente, nonché da un certificato di accreditamento, se disponibile, rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità è conforme ai requisiti di cui all'articolo 31.

Sono aggiunti documenti validi relativi alle designazioni esistenti dell'organismo notificato richiedente ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione.

3. Qualora non possa fornire un certificato di accreditamento, l'organismo di valutazione della conformità interessato fornisce all'autorità di notifica tutte le prove documentali necessarie per la verifica, il riconoscimento e il monitoraggio periodico della sua conformità ai requisiti di cui all'articolo 31.

4. Per gli organismi notificati designati ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione, tutti i documenti e i certificati connessi a tali designazioni possono essere utilizzati per sostenere e accelerare la loro procedura di designazione a norma del presente regolamento, a seconda dei casi.

Gli organismi notificati, designati ai sensi di una delle normative di armonizzazione dell'Unione elencate nell'allegato I, sezione A, che sono sottoposti alla procedura di valutazione unificata di cui all'articolo 28, paragrafo 8, presentano la domanda unica di valutazione all'autorità di notifica designata ai sensi di tale normativa di armonizzazione dell'Unione.

L'organismo notificato aggiorna la documentazione di cui ai paragrafi 2 e 3 del presente articolo ogni volta che si verificano cambiamenti di rilievo, al fine di consentire all'autorità responsabile degli organismi notificati di monitorare e verificare il continuo rispetto di tutte le prescrizioni di cui all'articolo 31.

ARTICOLO 30

Procedura di notifica

1. Le autorità di notifica possono notificare solo gli organismi di valutazione della conformità che siano conformi alle prescrizioni di cui all'articolo 31.

2. Le autorità di notifica notificano alla Commissione e agli altri Stati membri, sulla base dell'elenco dei codici, delle categorie e dei corrispondenti tipi di sistemi di IA di cui all'allegato XIV e utilizzando lo strumento elettronico di notifica elaborato e gestito dalla Commissione, ogni organismo di valutazione della conformità di cui al paragrafo 1.

Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato XIV, alla luce del progresso tecnico, dell'evoluzione delle conoscenze o di nuovi dati scientifici, aggiungendo all'elenco dei codici, delle categorie e dei corrispondenti tipi di sistemi di IA un nuovo codice, una nuova categoria o un nuovo tipo di sistema di IA, eliminando dall'elenco un codice, una categoria o un tipo di sistema di IA esistenti o spostando un codice o un tipo di sistema di IA da una categoria all'altra.

3. La notifica di cui al paragrafo 2 del presente articolo include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità, i tipi di sistemi di IA interessati, nonché la relativa attestazione di competenza. Qualora una notifica non sia basata su un certificato di accreditamento di cui all'articolo 29, paragrafo 2, l'autorità di notifica fornisce alla Commissione e

agli altri Stati membri le prove documentali che attestino la competenza dell'organismo di valutazione della conformità nonché le misure predisposte per fare in modo che tale organismo sia monitorato periodicamente e continui a soddisfare i requisiti di cui all'articolo 31.

4. L'organismo di valutazione della conformità interessato può eseguire le attività di un organismo notificato solo se non sono sollevate obiezioni da parte della Commissione o degli altri Stati membri entro due settimane dalla notifica da parte di un'autorità di notifica, qualora essa includa un certificato di accreditamento di cui all'articolo 29, paragrafo 2, o entro due mesi dalla notifica da parte dell'autorità di notifica, qualora essa includa le prove documentali di cui all'articolo 29, paragrafo 3.

5. Se sono sollevate obiezioni, la Commissione avvia senza ritardo consultazioni con gli Stati membri pertinenti e l'organismo di valutazione della conformità. Tenutone debito conto, la Commissione decide se l'autorizzazione è giustificata. La Commissione trasmette la propria decisione allo Stato membro interessato e all'organismo di valutazione della conformità pertinente.

ARTICOLO 31
Requisiti relativi agli organismi notificati
omissis

ARTICOLO 32
Presunzione di conformità ai requisiti relativi agli organismi notificati
omissis

ARTICOLO 33
Affiliate degli organismi notificati e subappaltatori
omissis

ARTICOLO 34
Obblighi operativi degli organismi notificati
omissis

ARTICOLO 35
Numeri di identificazione ed elenchi di organismi notificati
omissis

ARTICOLO 36
Modifiche delle notifiche
omissis

ARTICOLO 37
Contestazione della competenza degli organismi notificati
omissis

ARTICOLO 38
Coordinamento degli organismi notificati
omissis

ARTICOLO 39
Organismi di valutazione della conformità di paesi terzi
Gli organismi di valutazione della conformità istituiti a norma del diritto di un paese terzo con il quale l'Unione ha concluso un accordo possono essere autorizzati a svolgere le attività degli organismi notificati a norma del presente regolamento, a condizione che soddisfino i requisiti stabiliti all'articolo 31 o garantiscano un livello di conformità equivalente.

SEZIONE 5
Norme, valutazione della conformità, certificati, registrazione

ARTICOLO 40
Norme armonizzate e prodotti della normazione

1. I sistemi di IA ad alto rischio o i modelli di IA per finalità generali che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea conformemente al regolamento (UE) n. 1025/2012 si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, se del caso, agli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento, nella misura in cui tali requisiti o obblighi sono contemplati da tali norme.

2. In conformità dell'articolo 10 del regolamento (UE) n. 1025/2012, la Commissione presenta senza indebito ritardo richieste di normazione riguardanti tutti i requisiti di cui alla sezione 2 del presente capo e, se del caso, richieste di normazione riguardanti gli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento. La richiesta di normazione chiede inoltre prodotti relativi a processi di comunicazione e documentazione intesi a migliorare le prestazioni dei sistemi di IA in termini di risorse, come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e allo sviluppo efficiente sotto il profilo energetico dei modelli di IA per finalità generali. Nel preparare una richiesta di normazione, la Commissione consulta il consiglio per l'IA e i pertinenti portatori di interessi, compreso il forum consultivo.

Nel presentare una richiesta di normazione alle organizzazioni europee di normazione, la Commissione specifica che le norme devono essere chiare, coerenti, anche con le norme elaborate nei vari settori per i prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione elencata nell'allegato I, e volte a garantire che i sistemi di IA ad alto rischio o i modelli di IA per finalità generali immessi sul mercato o messi in servizio nell'Unione soddisfino i pertinenti requisiti od obblighi di cui al presente regolamento.

La Commissione chiede alle organizzazioni europee di normazione di dimostrare che si adoperano al massimo per conseguire gli obiettivi di cui al primo e al secondo comma del presente paragrafo conformemente all'articolo 24 del regolamento (UE) n. 1025/2012.

Conformemente al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e senza indebito ritardo, la Commissione chiede alle organiz-

zazioni europee di normazione di elaborare prodotti della normazione, comprese, se del caso, norme armonizzate, al fine di agevolare la conformità congiunta e la presunzione di conformità ai requisiti o agli obblighi di cui al capo III, sezioni 2 e 3, del presente regolamento e ai requisiti e agli obblighi pertinenti stabiliti nella normativa di armonizzazione dell'Unione elencata nell'allegato I del presente regolamento.

3. I partecipanti al processo di normazione cercano di promuovere gli investimenti e l'innovazione nell'IA, anche mediante una maggiore certezza del diritto, nonché la competitività e la crescita del mercato dell'Unione, di contribuire a rafforzare la cooperazione globale in materia di normazione e a tener conto delle norme internazionali esistenti nel settore dell'IA che sono coerenti con i valori, i diritti fondamentali e gli interessi dell'Unione, e di rafforzare la governance multipartecipativa garantendo una rappresentanza equilibrata degli interessi e l'effettiva partecipazione di tutti i portatori di interessi pertinenti conformemente agli articoli 5, 6 e 7 del regolamento (UE) n. 1025/2012.

ARTICOLO 41

Specifiche comuni

omissis

ARTICOLO 42

Presunzione di conformità a determinati requisiti

1. I sistemi di IA ad alto rischio che sono stati addestrati e sottoposti a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico all'interno del quale sono destinati a essere usati si presumono conformi ai pertinenti requisiti di cui all'articolo 10, paragrafo 4.

2. I sistemi di IA ad alto rischio che sono stati certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersicurezza a norma del regolamento (UE) 2019/881 e i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea si presumono conformi ai requisiti di cibersicurezza di cui all'articolo 15 del presente regolamento, nella misura in cui tali requisiti siano contemplati nel certificato di cibersicurezza o nella dichiarazione di conformità o in parti di essi.

3. Qualora i sistemi di IA ad alto rischio rientrino nell'ambito di applicazione del regolamento (UE) 2024/2847 e siano soddisfatte le condizioni di cui all'articolo 12, paragrafo 1, di tale regolamento, tali sistemi sono considerati conformi ai requisiti di cibersicurezza di cui all'articolo 15 del presente regolamento.

ARTICOLO 43

Valutazione della conformità

1. Per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, se ha applicato le norme armonizzate di cui all'articolo 40 o, ove applicabile, le specifiche comuni di cui all'articolo 41, nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, il fornitore sceglie una delle seguenti procedure di valutazione della conformità basate sugli elementi qui di seguito:

a) il controllo interno di cui all'allegato VI; oppure

b) la valutazione del sistema di gestione della qualità e la valutazione della documentazione tecnica, con il coinvolgimento di un organismo notificato, di cui all'allegato VII.

Nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII se:

a) non esistono le norme armonizzate di cui all'articolo 40 e non sono disponibili le specifiche comuni di cui all'articolo 41;

b) il fornitore non ha applicato la norma armonizzata o ne ha applicato solo una parte;

c) esistono le specifiche comuni di cui alla lettera a), ma il fornitore non le ha applicate;

d) una o più norme armonizzate di cui alla lettera a) sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione.

Ai fini della procedura di valutazione della conformità di cui all'allegato VII, il fornitore può scegliere uno qualsiasi degli organismi notificati. Tuttavia, se il sistema di IA ad alto rischio è destinato ad essere messo in servizio dalle autorità competenti in materia di contrasto, di immigrazione o di asilo, nonché da istituzioni, organi o organismi dell'Unione, l'autorità di vigilanza del mercato di cui all'articolo 74, paragrafo 8 o 9, a seconda dei casi, agisce in qualità di organismo notificato.

2. Per i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, i fornitori seguono la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI, che non prevede il coinvolgimento di un organismo notificato.

3. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fornitore del sistema segue la pertinente procedura di valutazione della conformità prevista conformemente alla pertinente normativa di armonizzazione dell'Unione. I requisiti di cui alla sezione 2 del presente capo si applicano a tali sistemi di IA ad alto rischio e fanno parte di tale valutazione. Si deve altresì procedere alla valutazione del sistema di gestione della qualità di cui all'articolo 17 e si applica l'allegato VII, punti 3, 4.3, 4.4 e 4.5, punto 4.6, quinto comma, e punto 5.

Ai fini di tale valutazione della conformità, gli organismi notificati che sono stati notificati ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, hanno la facoltà di valutare la conformità dei sistemi di IA ad alto rischio ai requisiti di cui alla sezione 2 del presente capo, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 31, paragrafi 4, 5, 10 e 11, sia stata valutata nel contesto della procedura di notifica conformemente alla pertinente normativa di armonizzazione dell'Unione, come comprovato dalla valutazione effettuata nell'ambito della notifica esistente. Fatto salvo l'articolo 28, tali organismi notificati che sono stati notificati ai sensi della normativa

di armonizzazione dell'Unione di cui all'allegato I, sezione A, presentano domanda di designazione conformemente alla sezione 4 del presente capo entro il 28 gennaio 2028.

Qualora la normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, offra al fabbricante del prodotto la facoltà di avvalersi di una valutazione della conformità che non comporti il coinvolgimento di terzi, purché abbia applicato le norme armonizzate per garantire la conformità a tutti i requisiti pertinenti, tale fabbricante può avvalersi di tale facoltà solo se ha applicato anche le norme armonizzate o, ove applicabili, le specifiche comuni di cui all'articolo 41, che contemplano tutti i requisiti di cui alla sezione 2 del presente capo. La classificazione di un prodotto come sistema di IA ad alto rischio conformemente all'articolo 6, paragrafo 1, non incide sulla scelta della procedura di valutazione della conformità prevista per i fabbricanti di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, compresa, se del caso, la possibilità di avvalersi di norme armonizzate. I fabbricanti di tali prodotti non sono tenuti a scegliere una procedura di valutazione della conformità che comporti la valutazione della conformità da parte di terzi solo a condizione che il prodotto includa un sistema di IA ad alto rischio come componente di sicurezza, se ciò non è richiesto dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A.

Se un sistema di IA ad alto rischio è disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, e rientra in una delle categorie elencate nell'allegato III, il fornitore di tale sistema segue la pertinente procedura di valutazione della conformità prevista ai sensi della pertinente normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A.

Ai fini di tale valutazione, gli organismi notificati che sono stati notificati a norma di tali atti giuridici hanno la facoltà di controllare la conformità dei sistemi di IA ad alto rischioai requisiti di cui alla sezione 2, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 31, paragrafi 4, 10 e 11, sia stata valutata nel contesto della procedura di notifica a norma di tali atti giuridici.

Qualora un atto giuridico elencato nell'allegato I, sezione A, consenta al fabbricante del prodotto di sottrarsi a una valutazione della conformitàda parte di terzi, purché abbia applicato tutte le norme armonizzate che contemplano tutti i requisiti pertinenti, tale fabbricante può avvalersi di tale facoltà solo se ha applicato anche le norme armonizzate o, ove applicabili, le specifiche comunidi cui all'articolo 41, che contemplano tutti i requisiti di cui alla sezione 2 del presente capo.

4. I sistemi di IA ad alto rischio che sono già stati oggetto di una procedura di valutazione della conformità sono sottoposti a una nuova procedura di valutazione della conformità nel caso di una modifica sostanziale, indipendentemente dal fatto che il sistema modificato sia destinato a essere ulteriormente distribuito o continui a essere usato dal deployer attuale.

Per i sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio, le modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità e fanno parte delle informazioni contenute nella documentazione tecnica di cui all'allegato IV, punto 2, lettera f), non costituiscono una modifica sostanziale.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare gli allegati VI e VII aggiornandoli alla luce del progresso tecnico.

6. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 che modificano i paragrafi 1 e 2 del presente articolo per assoggettare i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, alla procedura di valutazione della conformità di cui all'allegato VII o a parti di essa. La Commissione adotta tali atti delegati tenendo conto dell'efficacia della procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI nel prevenire o ridurre al minimo i rischi per la salute, la sicurezza e la protezione dei diritti fondamentali posti da tali sistemi, nonché della disponibilità di capacità e risorse adeguate tra gli organismi notificati.

ARTICOLO 44
Certificati
omissis

ARTICOLO 45
Obblighi di informazione degli organismi notificati
omissis

ARTICOLO 46
Deroga alla procedura di valutazione della conformità
omissis

ARTICOLO 47
Dichiarazione di conformità UE
omissis

ARTICOLO 48
Marcatura CE
omissis

ARTICOLO 49
Registrazione
omissis

CAPO IV
OBBLIGHI DI TRASPARENZA PER I FORNITORI E I DEPLOYER DI DETERMINATI SISTEMI DI IA

ARTICOLO 50
Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA

1. I fornitori garantiscono che i sistemi di IA destina-

ti a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. I fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente. I fornitori garantiscono che le loro soluzioni tecniche siano efficaci, interoperabili, solide e affidabili nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come eventualmente indicato nelle pertinenti norme tecniche. Tale obbligo non si applica se i sistemi di IA svolgono una funzione di assistenza per l'editing standard o non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica, o se autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati.

3. I deployer di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema e trattano i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680, a seconda dei casi. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica e il riconoscimento delle emozioni autorizzati dalla legge per accertare, prevenire o indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi e conformemente al diritto dell'Unione.

4. I deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «deep fake» rendono noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati. Qualora il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.

I deployer di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati o se il contenuto generato dall'IA è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.

5. Le informazioni di cui ai paragrafi da 1 a 4 sono fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione. Le informazioni devono essere conformi ai requisiti di accessibilità applicabili.

6. I paragrafi da 1 a 4 lasciano impregiudicati i requisiti e gli obblighi di cui al capo III, così come gli altri obblighi di trasparenza stabiliti dal diritto dell'Unione o nazionale per i deployer dei sistemi di IA.

7. La Commissione incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione, alla marcatura e all'etichettatura dei contenuti generati o manipolati artificialmente. La Commissione, tenendo nella massima considerazione il parere del consiglio per l'IA, valuta se l'adesione a tali codici di buone pratiche sia adeguata a garantire il rispetto degli obblighi di cui ai paragrafi 2 e 4 del presente articolo, secondo la procedura di cui all'articolo 56, paragrafo 6 . Se ritiene che il codice di buone pratiche non sia adeguato, la Commissione può adottare un atto di esecuzione che specifichi norme comuni per l'attuazione di tali obblighi secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

CAPO V
MODELLI DI IA PER FINALITÀ GENERALI

SEZIONE 1
Regole di classificazione

ARTICOLO 51
Classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischio sistemico

omissis

ARTICOLO 52
Procedura

omissis

SEZIONE 2
Obblighi dei fornitori di modelli di IA per finalità generali

ARTICOLO 53
Obblighi dei fornitori di modelli di IA per finalità generali

omissis

ARTICOLO 54
Rappresentanti autorizzati dei fornitori di modelli di IA per finalità generali

omissis

SEZIONE 3
Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico

ARTICOLO 55
Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico
omissis

SEZIONE 4
Codici di buone pratiche

ARTICOLO 56
Codici di buone pratiche

1. L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione al fine di contribuire alla corretta applicazione del presente regolamento, tenendo conto degli approcci internazionali.

2. L'ufficio per l'IA e il comitato mirano a garantire che i codici di buone pratiche contemplino almeno gli obblighi di cui agli articoli 53 e 55, compreso quanto segue:

a) i mezzi per garantire che le informazioni di cui all'articolo 53, paragrafo 1, lettere a) e b), siano mantenute aggiornate alla luce degli sviluppi tecnologici e di mercato;

b) un adeguato livello di dettaglio nella sintesi dei contenuti utilizzati per l'addestramento;

c) l'individuazione del tipo e della natura dei rischi sistemici a livello dell'Unione, comprese le rispettive fonti, se del caso;

d) le misure, le procedure e le modalità per la valutazione e la gestione dei rischi sistemici a livello dell'Unione, compresa la relativa documentazione, che devono essere proporzionate ai rischi e tenere conto della loro gravità e probabilità e delle sfide specifiche nell'affrontare tali rischi alla luce dei modi possibili in cui tali rischi possono emergere e concretizzarsi lungo la catena del valore dell'IA.

3. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali, nonché le pertinenti autorità nazionali competenti, a partecipare all'elaborazione dei codici di buone pratiche. Le organizzazioni della società civile, l'industria, il mondo accademico e altri pertinenti portatori di interessi, quali i fornitori a valle e gli esperti indipendenti, possono sostenere il processo.

4. L'ufficio per l'IA e il comitato mirano a garantire che i codici di buone pratiche definiscano chiaramente i loro obiettivi specifici e contengano impegni o misure, compresi, se del caso, indicatori chiave di prestazione, volti ad assicurare il conseguimento di tali obiettivi e che tengano debitamente conto delle esigenze e degli interessi di tutte le parti interessate, anche delle persone interessate, a livello dell'Unione.

5. L'ufficio per l'IA mira a garantire che i partecipanti all'elaborazione dei codici di buone pratiche riferiscano periodicamente all'ufficio per l'IA in merito all'attuazione degli impegni, alle misure adottate e ai loro esiti, anche rispetto agli indicatori chiave di prestazione, se del caso. Gli indicatori chiave di prestazione e gli impegni di comunicazione riflettono le differenze in termini di dimensioni e capacità tra i vari partecipanti.

6. La Commissione e il consiglio per l'IA monitorano e valutano periodicamente il conseguimento degli obiettivi dei codici di buone pratiche da parte dei partecipanti e il loro contributo alla corretta applicazione del presente regolamento. La Commissione, tenendo nella massima considerazione il parere del comitato, valuta se i codici di buone pratiche contemplano gli obblighi di cui agli articoli 53 e 55, e monitora e valuta periodicamente il conseguimento dei loro obiettivi. La Commissione pubblica la sua valutazione riguardante l'adeguatezza dei codici di buone pratiche.

La Commissione può approvare, mediante atto di esecuzione, un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

7. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali ad aderire ai codici di buone pratiche. Per i fornitori di modelli di IA per finalità generali che non presentano rischi sistemici, tale adesione può essere limitata agli obblighi di cui all'articolo 53, a meno che essi dichiarino esplicitamente il loro interesse ad aderire al codice nella sua interezza.

8. L'ufficio per l'IA incoraggia e agevola, se del caso, anche il riesame e l'adeguamento dei codici di buone pratiche, in particolare alla luce di norme emergenti. L'ufficio per l'IA fornisce assistenza per quanto riguarda la valutazione delle norme disponibili.

9. I codici di buone pratiche sono pronti al più tardi entro il 2 maggio 2025. L'ufficio per l'IA adotta le misure necessarie, compreso l'invito ai fornitori di cui al paragrafo 7.

Qualora entro il 2 agosto 2025, un codice di buone pratiche non possa essere portato a termine, o qualora l'ufficio per l'IA lo ritenga non adeguato a seguito della valutazione di cui al paragrafo 6 del presente articolo, la Commissione può prevedere, mediante atti di esecuzione, norme comuni per l'attuazione degli obblighi di cui agli articoli 53 e 55, comprese le questioni di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

CAPO VI
MISURE A SOSTEGNO DELL'INNOVAZIONE

ARTICOLO 57
Spazi di sperimentazione normativa per l'IA

1. Gli Stati membri provvedono affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sia operativo entro il 2 agosto 2027. Tale spazio di sperimentazione può essere inoltre istituito congiuntamente con le autorità competenti di altri Stati membri. La Commissione può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA.

L'obbligo di cui al primo comma può essere soddi-

sfatto anche partecipando a uno spazio di sperimentazione esistente nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti.

2. Possono essere altresì istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale, o congiuntamente con le autorità competenti di altri Stati membri.

3. Il Garante europeo della protezione dei dati può istituire uno spazio di sperimentazione normativa per l'IA per le istituzioni, gli organi e gli organismi dell'Unione. A tal fine, i riferimenti alle autorità nazionali competenti contenuti nel presente capo si intendono fatti al Garante europeo della protezione dei dati.

3 bis. L'ufficio per l'IA può istituire uno spazio di sperimentazione normativa per l'IA a livello dell'Unione per i sistemi di IA disciplinati dall'articolo 75, paragrafo 1. A tal fine, i riferimenti alle autorità nazionali competenti nel presente capo si intendono fatti, se del caso, all'ufficio per l'IA. Tale spazio di sperimentazione normativa per l'IA è posto in essere in stretta collaborazione con le pertinenti autorità competenti, in particolare se nello spazio di sperimentazione normativa per l'IA è oggetto di supervisione la conformità a atti normativi dell'Unione diversi dal presente regolamento, e garantisce un accesso prioritario alle PMI, comprese le start-up, e alle piccole imprese a media capitalizzazione.

L'istituzione, da parte dell'ufficio per l'IA, di uno spazio di sperimentazione normativa per l'IA a livello dell'Unione non pregiudica le competenze degli Stati membri di istituire e controllare spazi di sperimentazione normativa per l'IA per i sistemi di IA sotto la loro supervisione.

4. Gli Stati membri provvedono affinché le autorità competenti di cui ai paragrafi 1 e 2 assegnino risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva. Se del caso, le autorità nazionali competenti cooperano con altre autorità pertinenti e possono consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA. Il presente articolo lascia impregiudicati gli altri spazi di sperimentazione normativa istituiti a norma del diritto dell'Unione o nazionale. Gli Stati membri garantiscono un livello adeguato di cooperazione tra le autorità che controllano tali altri spazi di sperimentazione e le autorità nazionali competenti.

5. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del presente articolo garantiscono un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e le autorità competenti, assicurando che siano predisposte garanzie adeguate. Tali spazi di sperimentazione possono comprendere prove in condizioni reali soggette a controllo nei medesimi spazi. Se del caso, il piano dello spazio di sperimentazione include il piano di prova in condizioni reali di cui agli articoli 60 e 60-bis.

6. Le autorità competenti, se del caso, forniscono orientamenti e garantiscono il controllo e il sostegno nell'ambito dello spazio di sperimentazione normativa per l'IA al fine di individuare i rischi, in particolare per quanto riguarda i diritti fondamentali, la salute e la sicurezza, le prove, le misure di attenuazione e la loro efficacia, in relazione agli obblighi e ai requisiti del presente regolamento e, se del caso, di altre disposizioni del diritto dell'Unione e nazionale, la conformità ai quali è soggetta a controllo nell'ambito dello spazio di sperimentazione.

7. Le autorità competenti forniscono ai fornitori e ai potenziali fornitori che partecipano allo spazio di sperimentazione normativa per l'IA orientamenti sulle aspettative normative e sulle modalità per soddisfare i requisiti e gli obblighi di cui al presente regolamento.

Su richiesta del fornitore o del potenziale fornitore del sistema di IA, l'autorità competente fornisce una prova scritta delle attività svolte con successo nello spazio di sperimentazione. L'autorità competente fornisce inoltre una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione e i relativi risultati e le conclusioni dell'apprendimento. I fornitori possono utilizzare tale documentazione per dimostrare la loro conformità al presente regolamento attraverso la procedura di valutazione della conformità o le pertinenti attività di vigilanza del mercato. A tale riguardo, la relazione di uscita e la prova scritta fornite dall'autorità nazionale competente sono prese favorevolmente in considerazione dalle autorità di vigilanza del mercato e dagli organismi notificati, al fine di accelerare le procedure di valutazione della conformità in misura ragionevole.

8. Fatte salve le disposizioni in materia di riservatezza di cui all'articolo 78, e con l'accordo del fornitore o del potenziale fornitore, la Commissione e il comitato sono autorizzati ad accedere alle relazioni di uscita e ne tengono conto, se del caso, nell'esercizio dei loro compiti a norma del presente regolamento. Se sia il fornitore o il potenziale fornitore sia l'autorità nazionale competente acconsentono esplicitamente, la relazione di uscita può essere messa a disposizione del pubblico attraverso la piattaforma unica di informazione di cui al presente articolo.

9. L'istituzione di spazi di sperimentazione normativa per l'IA mira a contribuire agli obiettivi seguenti:

a) migliorare la certezza del diritto al fine di conseguire la conformità normativa al presente regolamento o, se del caso, ad altre applicabili disposizioni di diritto dell'Unione e nazionale;

b) sostenere la condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA;

c) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA;

d) contribuire all'apprendimento normativo basato su dati concreti;

e) agevolare e accelerare l'accesso al mercato

dell'Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up, e dalle piccole imprese a media capitalizzazione.

10. Le autorità nazionali competenti garantiscono che, nella misura in cui i sistemi di IA innovativi comportano il trattamento di dati personali o rientrano altrimenti nell'ambito di competenza di altre autorità nazionali o autorità competenti che forniscono o sostengono l'accesso ai dati, le autorità competenti per la protezione dei dati e tali altre autorità nazionali o competenti siano associate al funzionamento dello spazio di sperimentazione normativa per l'IA e partecipino al controllo di tali aspetti nei limiti dei rispettivi compiti e poteri.

11. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi o di controllo delle autorità competenti che controllano gli spazi di sperimentazione, anche a livello regionale o locale. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi di IA comporta adeguate misure di attenuazione. Le autorità nazionali competenti hanno il potere di sospendere, in via temporanea o permanente, il processo di prova o la partecipazione allo spazio di sperimentazione, se non è possibile un'attenuazione efficace, e informano l'ufficio per l'IA di tale decisione. Le autorità nazionali competenti esercitano i loro poteri di controllo entro i limiti del pertinente diritto, utilizzando i loro poteri discrezionali nell'attuazione delle disposizioni giuridiche per quanto riguarda uno specifico progetto di spazio di sperimentazione normativa per l'IA, con l'obiettivo di promuovere l'innovazione nell'IA nell'Unione.

12. I fornitori e i potenziali fornitori partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. Tuttavia, a condizione che i potenziali fornitori rispettino il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di violazione del presente regolamento. Qualora altre autorità competenti responsabili del diritto dell'Unione e nazionale abbiano partecipato attivamente al controllo del sistema di IA nello spazio di sperimentazione e abbiano fornito orientamenti ai fini della conformità, nessuna sanzione amministrativa pecuniaria è inflitta in relazione a tali disposizioni di diritto.

13. Gli spazi di sperimentazione normativa per l'IA sono progettati e attuati in modo tale da agevolare, se del caso, la cooperazione transfrontaliera tra le autorità nazionali competenti.

14. Le autorità nazionali competenti, il Garante europeo della protezione dei dati e l'ufficio per l'IA, se del caso e nell'ambito delle rispettive competenze, coordinano le loro attività e cooperano nel quadro del comitato. Essi possono sostenere l'istituzione e il funzionamento congiunti degli spazi di sperimentazione normativa per l'IA, anche in settori diversi, e scambiare le migliori pratiche in materia.

15. Le autorità nazionali competenti informano l'ufficio per l'IA e il comitato di uno spazio di sperimentazione e possono chiedere sostegno e orientamenti. L'ufficio per l'IA mette a disposizione del pubblico l'elenco degli spazi di sperimentazione normativa pianificati ed esistenti e lo mantiene aggiornato al fine di incoraggiare una maggiore interazione negli spazi di sperimentazione e nella cooperazione transfrontaliera.

16. Le autorità nazionali competenti presentano relazioni annuali all'ufficio per l'IA e al comitato a decorrere dall'anno successivo all'istituzione dello spazio di sperimentazione normativa per l'IA e successivamente ogni anno fino alla sua cessazione, nonché una relazione definitiva. Tali relazioni contengono informazioni sui progressi e sui risultati dell'attuazione di tali spazi di sperimentazione, comprese le migliori pratiche, gli incidenti, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione ed eventuale revisione del presente regolamento, inclusi i rispettivi atti delegati e di esecuzione, e sull'applicazione di altre disposizioni di diritto dell'Unione soggette a controllo da parte delle autorità competenti nell'ambito dello spazio di sperimentazione. Le autorità nazionali competenti mettono tali relazioni annuali o estratti delle stesse a disposizione del pubblico online. La Commissione tiene conto, se del caso, delle relazioni annuali nell'esercizio dei suoi compiti a norma del presente regolamento.

17. La Commissione sviluppa un'interfaccia unica e dedicata contenente tutte le informazioni pertinenti relative agli spazi di sperimentazione normativa per l'IA per permettere ai portatori di interessi di interagire con gli spazi di sperimentazione normativa per l'IA e di formulare richieste di informazioni presso le autorità competenti e di chiedere orientamenti non vincolanti sulla conformità di prodotti, servizi e modelli aziendali innovativi che integrano le tecnologie di IA, a norma dell'articolo 62, paragrafo 1, lettera c). La Commissione si coordina proattivamente con le autorità nazionali competenti, se del caso.

ARTICOLO 58

Modalità dettagliate e funzionamento degli spazi di sperimentazione normativa per l'IA

1. Onde evitare la frammentazione nell'intera Unione, la Commissione adotta atti di esecuzione che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento, la governance e la supervisione degli spazi di sperimentazione normativa per l'IA. Tali atti di esecuzione comprendono principi comuni sulle questioni seguenti:

a) criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA;

b) procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita;

c) i termini e le condizioni applicabili ai partecipanti;

d) le norme dettagliate applicabili alla governance degli spazi di sperimentazione normativa per l'IA di cui all'articolo 57, anche per quanto riguarda il coinvolgimento delle autorità di protezione dei dati competenti e la supervisione da esse esercitata, ove pertinente, e il coordinamento e la cooperazione a livello nazionale e dell'Unione.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Gli atti di esecuzione di cui al paragrafo 1 garantiscono:

a) che gli spazi di sperimentazione normativa per l'IA siano aperti a qualsiasi fornitore o potenziale fornitore richiedente di un sistema di IA che soddisfi criteri di ammissibilità e selezione trasparenti ed equi, e che le autorità nazionali competenti informino i richiedenti della loro decisione entro tre mesi dalla domanda;

b) che gli spazi di sperimentazione normativa consentano un accesso ampio e paritario e tengano il passo con la domanda di partecipazione; i fornitori e i potenziali fornitori possono anche presentare domande in partenariato con gli deployers e con altri terzi interessati;

c) che le modalità dettagliate e le condizioni relative agli spazi di sperimentazione normativa per l'IA sostengano la flessibilità, nella massima misura possibile, affinché le autorità nazionali competenti istituiscano e gestiscano i loro spazi di sperimentazione normativa per l'IA;

d) che l'accesso agli spazi di sperimentazione normativa per l'IA sia gratuito per le PMI, comprese le start-up, fatti salvi i costi straordinari che le autorità nazionali competenti possono recuperare in maniera equa e proporzionata;

e) che i fornitori e i potenziali fornitori siano agevolati, attraverso i risultati dell'apprendimento degli spazi di sperimentazione normativa per l'IA, a conformarsi agli obblighi di valutazione della conformità di cui al presente regolamento e all'applicazione volontaria dei codici di condotta di cui all'articolo 95;

f) che gli spazi di sperimentazione normativa per l'IA facilitino il coinvolgimento di altri attori pertinenti nell'ambito dell'ecosistema dell'IA, quali organismi notificati e organizzazioni di normazione, PMI, comprese start-up, imprese, innovatori, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione e poli europei dell'innovazione digitale, centri di eccellenza e singoli ricercatori, al fine di consentire e facilitare la cooperazione con i settori pubblico e privato;

g) che le procedure, i processi e i requisiti amministrativi per l'applicazione, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione normativa per l'IA siano semplici, facilmente intelligibili, comunicati chiaramente per agevolare la partecipazione delle PMI, comprese le start-up, con capacità giuridiche e amministrative limitate e siano razionalizzati in tutta l'Unione, al fine di evitare la frammentazione e che la partecipazione a uno spazio di sperimentazione normativa per l'IA istituito da uno Stato membro o dal Garante europeo della protezione dei dati sia reciprocamente e uniformemente riconosciuta e produca gli stessi effetti giuridici nell'intera Unione;

h) che la partecipazione allo spazio di sperimentazione normativa per l'IA sia limitata a un periodo adeguato alla complessità e alla portata del progetto, che può essere prorogato dall'autorità nazionale competente;

i) che gli spazi di sperimentazione normativa per l'IA agevolino lo sviluppo di strumenti e infrastrutture per la sperimentazione, l'analisi comparativa, la valutazione e la spiegazione delle dimensioni dei sistemi di IA pertinenti per l'apprendimento normativo, quali l'accuratezza, la robustezza e la cibersicurezza, nonché le misure per attenuare i rischi per i diritti fondamentali e la società in generale.

3. I potenziali fornitori degli spazi di sperimentazione normativa per l'IA, soprattutto le PMI e le start-up, sono indirizzati, se del caso, a servizi di pre-diffusione, quali gli orientamenti sull'attuazione del presente regolamento, ad altri servizi a valore aggiunto, quali l'assistenza per i documenti di normazione e la certificazione, gli impianti di prova e sperimentazione, i poli europei dell'innovazione digitale e i centri di eccellenza.

4. Quando valutano la possibilità di autorizzare prove in condizioni reali sottoposte a controllo nel quadro di uno spazio di sperimentazione normativa per l'IA da istituire a norma del presente articolo, le autorità nazionali competenti concordano in modo specifico con i partecipanti i termini e le condizioni di tali prove e, in particolare, le tutele adeguate al fine di proteggere i diritti fondamentali, la salute e la sicurezza. Se del caso, cooperano con altre autorità nazionali competenti al fine di garantire pratiche coerenti in tutta l'Unione.

ARTICOLO 59

Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico

omissis

ARTICOLO 60

Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Le prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA possono essere effettuate da fornitori o potenziali fornitori di sistemi di IA ad alto rischio elencati nell'allegato III o disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, conformemente al presente articolo e al piano di prova in condizioni reali di cui al presente articolo, fatti salvi i divieti di cui all'articolo 5.

La Commissione, per mezzo di atti di esecuzione, specifica nel dettaglio gli elementi del piano di prova in condizioni reali. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Il presente paragrafo lascia impregiudicato il diritto dell'Unione o nazionale concernente le prove in condizioni reali di sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I.

2. I fornitori o potenziali fornitori possono effettuare prove dei sistemi di IA ad alto rischio di cui all'allegato III o disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, in condizioni reali in qualsiasi momento prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, da soli o in partenariato con uno o più deployer o potenziali deployer.

3. Le prove di sistemi di IA ad alto rischio in condizioni reali a norma del presente articolo non pregiudicano alcun esame etico che sia richiesto dal diritto dell'Unione o nazionale.

4. I fornitori o potenziali fornitori possono effettuare le prove in condizioni reali solo se sono soddisfatte tutte le condizioni seguenti:

a) il fornitore o potenziale fornitore ha elaborato un piano di prova in condizioni reali e lo ha presentato all'autorità di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali;

b) l'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali ha approvato le prove in condizioni reali e il piano di prova in condizioni reali; se l'autorità di vigilanza del mercato non ha fornito una risposta entro 30 giorni, le prove in condizioni reali e il piano di prova in condizioni reali sono da intendersi approvati; se il diritto nazionale non prevede un'approvazione tacita, le prove in condizioni reali restano soggette ad autorizzazione;

c) il fornitore o potenziale fornitore, ad eccezione dei fornitori o dei potenziali fornitori dei sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, e dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 71, paragrafo 4, con un numero di identificazione unico a livello dell'Unione e con le informazioni di cui all'allegato IX; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori dell'attività di contrasto, della migrazione, dell'asilo e della gestione del controllo di frontiera, ha registrato la prova in condizioni reali in una sezione sicura non pubblica della banca dati UE ai sensi dell'articolo 49, paragrafo 4, lettera d), con un numero di identificazione unico a livello dell'Unione e con le informazioni ivi specificate; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 49, paragrafo 5;

d) il fornitore o potenziale fornitore che effettua le prove in condizioni reali è stabilito nell'Unione o ha nominato un rappresentante legale che è stabilito nell'Unione;

e) i dati raccolti e trattati ai fini delle prove in condizioni reali sono trasferiti a paesi terzi solo a condizione che siano poste in essere tutele adeguate e applicabili ai sensi del diritto dell'Unione;

f) le prove in condizioni reali non durano più di quanto necessario per conseguire i rispettivi obiettivi e, in ogni caso, non più di sei mesi, che possono essere prorogati per un ulteriore periodo di sei mesi, previa notifica da parte del fornitore o del potenziale fornitore all'autorità di vigilanza del mercato, corredata della motivazione relativa alla necessità di tale proroga;

g) i soggetti delle prove in condizioni reali che sono persone appartenenti a gruppi vulnerabili a causa della loro età o disabilità sono adeguatamente protetti;

h) qualora un fornitore o potenziale fornitore organizzi le prove in condizioni reali in cooperazione con uno o più deployer o potenziali deployer, questi ultimi sono stati informati di tutti gli aspetti delle prove pertinenti per la loro decisione di partecipare e hanno ricevuto le istruzioni pertinenti per l'uso del sistema di IA di cui all'articolo 13; il fornitore o potenziale fornitore e il deployer o potenziale deployer concludono un accordo che ne specifica i ruoli e le responsabilità al fine di garantire la conformità alle disposizioni relative alle prove in condizioni reali ai sensi del presente regolamento e di altre disposizioni applicabili di diritto dell'Unione e nazionale;

i) i soggetti delle prove in condizioni reali hanno dato il proprio consenso informato a norma dell'articolo 61 o, nel caso delle attività di contrasto, qualora la richiesta di consenso informato impedisca di sottoporre a prova il sistema di IA, le prove stesse e i risultati delle prove in condizioni reali non hanno alcun effetto negativo sui soggetti e i loro dati personali sono cancellati dopo lo svolgimento della prova;

j) le prove in condizioni reali sono efficacemente supervisionate dal fornitore o potenziale fornitore, nonché dai deployer o dai potenziali deployer, tramite persone adeguatamente qualificate nel settore pertinente e dotate delle capacità, della formazione e dell'autorità necessarie per svolgere i loro compiti;

k) le previsioni, le raccomandazioni o le decisioni del sistema di IA possono essere efficacemente ribaltate e ignorate.

5. Qualsiasi soggetto delle prove in condizioni reali, o il suo rappresentante legale designato, a seconda dei casi, può, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione, ritirarsi dalle prove in qualsiasi momento revocando il proprio consenso informato e può chiedere la cancellazione immediata e permanente dei propri dati personali. La revoca del consenso informato non pregiudica le attività già svolte.

6. A norma dell'articolo 75, gli Stati membri conferiscono alle loro autorità di vigilanza del mercato il potere di imporre ai fornitori e ai potenziali fornitori di fornire informazioni, di effettuare ispezioni a distanza o in loco senza preavviso e di svolgere controlli sulla conduzione delle prove in condizioni reali e sui relativi sistemi di IA ad alto rischio. Le autorità di vigilanza del

mercato si avvalgono di tali poteri per garantire lo sviluppo in sicurezza delle prove in condizioni reali.

7. Qualsiasi incidente grave individuato nel corso delle prove in condizioni reali è segnalato all'autorità nazionale di vigilanza del mercato conformemente all'articolo 73. Il fornitore o potenziale fornitore adotta misure di attenuazione immediate o, in mancanza di ciò, sospende le prove in condizioni reali fino a quando tale attenuazione non abbia luogo oppure vi pone fine. Il fornitore o potenziale fornitore stabilisce una procedura per il tempestivo ritiro del sistema di IA in seguito a tale cessazione delle prove in condizioni reali.

8. I fornitori o potenziali fornitori notificano all'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali la sospensione o la cessazione delle prove in condizioni reali nonché i risultati finali.

9. Il fornitore o potenziale fornitore è responsabile ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni causati nel corso delle prove in condizioni reali.

ARTICOLO 60 BIS

Prove di sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Gli Stati membri possono consentire, conformemente al presente articolo, lo svolgimento di prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA da parte di fornitori o potenziali fornitori di prodotti basati sull'IA disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, al fine di valutare e verificare la conformità di tali sistemi ai requisiti di cui agli articoli da 8 a 15.

2. Gli Stati membri che scelgono di consentire lo svolgimento di prove di cui al paragrafo 1 adottano, individualmente o congiuntamente, quadri per le prove in condizioni reali.

3. Ciascuno Stato membro notifica alla Commissione qualsiasi quadro per le prove in condizioni reali che adotta prima di attuarlo. Ciò non pregiudica le competenze della Commissione ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B.

4. Gli Stati membri che hanno adottato quadri per le prove in condizioni reali garantiscono che le autorità nazionali competenti, le autorità pertinenti e le autorità pubbliche responsabili della gestione e del funzionamento delle infrastrutture e dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, cooperino strettamente e in buona fede tra loro e rimuovano qualsiasi ostacolo pratico, anche per quanto riguarda le norme procedurali che disciplinano l'accesso alle infrastrutture pubbliche fisiche, ove necessario, al fine di applicare con efficacia tali quadri relativi alle prove in condizioni reali e di effettuare prove sui prodotti basati sull'IA disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I.

5. I quadri per le prove in condizioni reali stabiliscono i requisiti in base ai quali si effettuano le prove in condizioni reali. Tali quadri:

a) prevedono la presentazione di un piano obbligatorio di prove in condizioni reali da concordare tra il fornitore o potenziale fornitore e l'autorità nazionale competente o l'autorità pertinente conformemente alla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B;

b) garantiscono la conformità alle prescrizioni di cui all'articolo 60, paragrafi 2 e 3, paragrafo 4, lettere da d) a j), e paragrafi da 5 a 9, laddove qualsiasi riferimento alle autorità di vigilanza del mercato in tali disposizioni si intenda fatto all'autorità nazionale competente o all'autorità pertinente, a seconda dei casi, conformemente alla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B;

c) includono disposizioni efficaci in materia di governance e assunzione di responsabilità;

d) garantiscono un elevato livello di protezione della salute e della sicurezza e dei diritti fondamentali.

6. Le prove in condizioni reali sono conformi alle disposizioni applicabili stabilite nella normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B. I requisiti stabiliti in tali disposizioni non pregiudicano l'applicazione del presente articolo nella misura necessaria a consentire lo svolgimento delle prove di cui al paragrafo 1.

ARTICOLO 61

Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

omissis

ARTICOLO 62

Misure per i fornitori e i deployer, in particolare le PMI, comprese le start-up

omissis

ARTICOLO 63

Deroghe per operatori specifici

1. Le PMI, comprese le start-up, possono conformarsi a determinati elementi del sistema di gestione della qualità di cui all'articolo 17 in modo semplificato, purché non abbiano imprese associate o collegate ai sensi della raccomandazione 2003/361/CE. A tal fine, la Commissione elabora orientamenti sugli elementi del sistema di gestione della qualità che possono essere rispettati in modo semplificato tenendo conto delle esigenze delle PMI, senza incidere sul livello di protezione o sulla necessità di conformità ai requisiti per quanto riguarda i sistemi di IA ad alto rischio.

2. Il paragrafo 1 del presente articolo non è interpretato nel senso che esenta tali operatori dal rispetto di altri requisiti e obblighi di cui al presente regolamento, compresi quelli stabiliti agli articoli 9, 10, 11, 12, 13, 14, 15, 72 e 73.

CAPO VII
GOVERNANCE

SEZIONE 1
Governance a livello dell'Unione

ARTICOLO 64
Ufficio per l'IA

1. La Commissione sviluppa le competenze e le capacità dell'Unione nel settore dell'IA attraverso l'ufficio per l'IA.

2. Gli Stati membri agevolano i compiti affidati all'ufficio per l'IA, come indicato nel presente regolamento.

3. Fatta salva la procedura di bilancio, all'ufficio per l'IA sono assegnate risorse adeguate per svolgere efficacemente le proprie funzioni ed esercitare i propri poteri in relazione all'esecuzione del presente regolamento.

ARTICOLO 65
Istituzione e struttura del consiglio per l'IA europeo per l'intelligenza artificiale

omissis

ARTICOLO 66
Compiti del consiglio per l'IA

omissis

ARTICOLO 67
Forum consultivo

omissis

ARTICOLO 68
Gruppo di esperti scientifici indipendenti

omissis

ARTICOLO 69
Accesso al gruppo di esperti da parte degli Stati membri

1. Gli Stati membri possono ricorrere agli esperti scientifici del gruppo affinché sostengano le loro attività di esecuzione a norma del presente regolamento.

2. Gli Stati membri possono essere tenuti a pagare tariffe per la consulenza e il sostegno forniti dagli esperti a un tasso equivalente alle tariffe di retribuzione applicabili alla Commissione ai sensi dell'atto di esecuzione di cui all'articolo 68, paragrafo 1.

3. La Commissione facilita l'accesso tempestivo agli esperti da parte degli Stati membri, ove necessario, e garantisce che la combinazione di attività di sostegno svolte dalle strutture di sostegno dell'Unione per la prova dell'IA a norma dell'articolo 84 e dagli esperti a norma del presente articolo sia organizzata in modo efficiente e fornisca il miglior valore aggiunto possibile.

SEZIONE 2
Autorità nazionali competenti

ARTICOLO 70
Designazione delle autorità nazionali competenti e dei punti di contatto unici

1. Ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro.

2. Gli Stati membri comunicano alla Commissione l'identità delle autorità di notifica e delle autorità di vigilanza del mercato e i compiti di tali autorità, nonché ogni successiva modifica degli stessi. Gli Stati membri mettono a disposizione del pubblico le informazioni sulle modalità con cui le autorità competenti e i punti di contatto unici possono essere contattati, tramite mezzi di comunicazione elettronica, entro il 2 agosto 2025. Gli Stati membri designano un'autorità di vigilanza del mercato che funga da punto di contatto unico per il presente regolamento e notificano alla Commissione l'identità del punto di contatto unico. La Commissione elabora un elenco dei punti di contatto unici disponibili al pubblico.

3. Gli Stati membri garantiscono che le loro autorità nazionali competenti dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti a norma del presente regolamento. In particolare, le autorità nazionali competenti dispongono 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 cibersicurezza, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti. Gli Stati membri valutano e, se necessario, aggiornano annualmente i requisiti in termini di competenze e risorse di cui al presente paragrafo.

4. Le autorità nazionali competenti adottano misure adeguate per garantire un livello adeguato di cibersicurezza.

5. Nello svolgimento dei propri compiti, le autorità nazionali competenti agiscono in conformità degli obblighi di riservatezza di cui all'articolo 78.

6. Entro il 2 agosto 2025, e successivamente una volta ogni due anni, gli Stati membri riferiscono alla Commissione in merito allo stato delle risorse finanziarie e umane delle autorità nazionali competenti, con una valutazione della loro adeguatezza. La Commissione trasmette tali informazioni al consiglio per l'IA affinché le discuta e formuli eventuali raccomandazioni.

7. La Commissione agevola lo scambio di esperienze tra autorità nazionali competenti.

8. Le autorità nazionali competenti possono fornire orientamenti e consulenza sull'attuazione del presente regolamento, in particolare alle PMI, comprese le start-up, e alle piccole imprese a media capitalizzazio-

ne, tenendo conto degli orientamenti e della consulenza del consiglio per l'IA e della Commissione, a seconda dei casi. Ogniqualvolta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre disposizioni di diritto dell'Unione, sono consultate le autorità nazionali competenti a norma di tali disposizioni di diritto dell'Unione, come opportuno.

9. Qualora le istituzioni, gli organi e gli organismi dell'Unione rientrino nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità competente per la loro vigilanza.

CAPO VIII
BANCA DATI DELL'UE PER I SISTEMI DI IA AD ALTO RISCHIO

ARTICOLO 71

Banca dati dell'UE per i sistemi di IA ad alto rischio elencati nell'allegato III

omissis

CAPO IX
MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO, CONDIVISIONE DELLE INFORMAZIONI E VIGILANZA DEL MERCATO

SEZIONE 1

Monitoraggio successivo all'immissione sul mercato

ARTICOLO 72

Monitoraggio successivo all'immissione sul mercato effettuato dai fornitori e piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio

1. I fornitori istituiscono e documentano un sistema di monitoraggio successivo all'immissione sul mercato che sia proporzionato alla natura delle tecnologie di IA e ai rischi del sistema di IA ad alto rischio.

2. Il sistema di monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza attivamente e sistematicamente i dati pertinenti che possono essere forniti dai deployer o che possono essere raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la costante conformità dei sistemi di IA ai requisiti di cui al capo III, sezione 2. Se del caso, il monitoraggio successivo all'immissione sul mercato include un'analisi dell'interazione con altri sistemi di IA. Tale obbligo non riguarda i dati operativi sensibili dei deployer che sono autorità di contrasto.

3. Il sistema di monitoraggio successivo all'immissione sul mercato si basa su un piano di monitoraggio successivo all'immissione sul mercato. Il piano di monitoraggio successivo all'immissione sul mercato fa parte della documentazione tecnica di cui all'allegato IV. La Commissione, tenendo nella massima considerazione il parere del consiglio per l'IA, adotta orientamenti, compreso un modello, sul piano di monitoraggio successivo all'immissione sul mercato entro il 2 settembre 2027.

4. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora tale normativa preveda già un sistema e un piano di monitoraggio successivo all'immissione sul mercato, al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari elementi di cui ai paragrafi 1, 2 e 3 utilizzando il modello di cui al paragrafo 3 nei sistemi e nei piani già esistenti in virtù di tale normativa, a condizione che consegua un livello di protezione equivalente.

Il primo comma del presente paragrafo si applica anche ai sistemi di IA ad alto rischio di cui all'allegato III, punto 5, immessi sul mercato o messi in servizio da istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari.

SEZIONE 2

Condivisione di informazioni su incidenti gravi

ARTICOLO 73

Comunicazione di incidenti gravi

omissis

SEZIONE 3

Applicazione

ARTICOLO 74

Vigilanza del mercato e controllo dei sistemi di IA nel mercato dell'Unione

omissis

ARTICOLO 75

Vigilanza del mercato e controllo dei sistemi di IA e assistenza reciproca

1. L'ufficio per l'IA ha competenza esclusiva per il controllo e l'esecuzione degli obblighi a norma del presente regolamento in relazione ai sistemi di IA seguenti:

a) sistemi di IA basati su modelli di IA per finalità generali qualora il modello e il sistema siano sviluppati dallo stesso fornitore o da fornitori che fanno parte della stessa impresa di tale fornitore, ad eccezione di:

i) sistemi di IA relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

ii) sistemi di IA di cui all'allegato III, punto 2;

iii) sistemi di IA forniti dalle autorità di contrasto, dalle autorità di gestione delle frontiere e dagli istituti finanziari, nella misura in cui tali sistemi di IA rientrano nell'ambito di applicazione dell'articolo 74, paragrafo 6; e

iv) sistemi di IA di cui all'allegato III, punto 8, per quanto riguarda l'amministrazione della giustizia;

b) sistemi di IA che costituiscono o sono integrati in

piattaforme online di dimensioni molto grandi designate o motori di ricerca online di dimensioni molto grandi designati conformemente al regolamento (UE) 2022/2065.

La competenza esclusiva di cui al primo comma si applica ai fornitori di tali sistemi. Si applica ai deployer di tali sistemi solo se sono anche il fornitore o fanno parte della stessa impresa del fornitore.

1-bis. In deroga all'articolo 73, i fornitori di sistemi di IA ad alto rischio, di competenza dell'ufficio per l'IA a norma del paragrafo 1 del presente articolo, segnalano eventuali incidenti gravi all'ufficio per l'IA. L'articolo 73, paragrafi da 2 a 9, si applica mutatis mutandis. L'ufficio per l'IA trasmette tempestivamente le informazioni pertinenti all'autorità di vigilanza del mercato dello Stato membro nel cui territorio è situato il fornitore o il suo rappresentante legale.

1-ter. Le autorità coinvolte nell'applicazione del presente regolamento cooperano attivamente con l'ufficio per l'IA e gli prestano l'assistenza necessaria per l'esercizio dei suoi poteri, anche, se necessario, in relazione alle ispezioni o ad altre misure di esecuzione poste in essere nel territorio di uno Stato membro. A tal fine, tali autorità dispongono dei poteri previsti dal presente regolamento e dal regolamento (UE) 2019/1020 e, se del caso e nei limiti di quanto necessario per lo svolgimento dei loro compiti a norma del presente paragrafo, conformemente alle procedure nazionali applicabili.

1-quater. Quando adotta misure di indagine o esecuzione nel territorio di uno Stato membro che comportano l'accesso ai dati o al sistema di IA di un'autorità pubblica, l'ufficio per l'IA è assistito dalla pertinente autorità di vigilanza del mercato.

1-quinquies. Prima di adottare una decisione che avrebbe l'effetto di vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA su un mercato nazionale, o una decisione di ritirare o richiamare il sistema di IA da tale mercato, l'ufficio per l'IA notifica, senza indebito ritardo, l'autorità di vigilanza del mercato competente per tale mercato della sua intenzione di adottare una siffatta decisione. L'ufficio per l'IA consulta le autorità coinvolte nell'applicazione del presente regolamento, se del caso, su qualsiasi questione relativa all'applicazione e all'esecuzione del presente regolamento.

1 sexies. L'ufficio per l'IA è responsabile delle valutazioni della conformità e delle prove dei sistemi di IA di cui al paragrafo 1 del presente articolo che sono classificati come ad alto rischio e sottoposti a una valutazione di conformità da parte di terzi a norma dell'articolo 43, prima che tali sistemi di IA siano immessi sul mercato o messi in servizio. Tali prove e valutazioni verificano che i sistemi siano conformi ai pertinenti requisiti del presente regolamento e possano essere immessi sul mercato o messi in servizio nell'Unione in conformità del presente regolamento. La Commissione affida l'esecuzione di tali prove o valutazioni a organismi notificati designati in conformità del presente regolamento, nel qual caso l'organismo notificato agisce per conto della Commissione. Se un organismo notificato cui la Commissione ha delegato compiti a norma del presente paragrafo non li svolge adeguatamente, la Commissione può revocare la delega con effetto immediato.

Le tariffe per le attività di prova e valutazione sono a carico del fornitore del sistema di IA ad alto rischio che ha presentato alla Commissione la domanda di valutazione della conformità da parte di terzi. Il fornitore paga direttamente all'organismo notificato i costi relativi ai servizi affidati dalla Commissione agli organismi notificati in conformità del presente articolo.

2. Qualora abbiano motivi sufficienti per ritenere che i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai deployer per almeno una finalità classificata come ad alto rischio a norma del presente regolamento non siano conformi ai requisiti di cui al presente regolamento, le pertinenti autorità di vigilanza del mercato cooperano con l'ufficio per l'IA per effettuare valutazioni della conformità e informano di conseguenza il consiglio per l'IA e le altre autorità di vigilanza del mercato.

2 bis. Qualora abbia motivi fondati e sufficienti di sospettare che un fornitore o un deployer di un sistema di IA di cui al paragrafo 1 del presente articolo abbia violato il presente regolamento, un'autorità di vigilanza del mercato può chiedere all'ufficio per l'IA, attraverso il pertinente punto di contatto unico designato in conformità dell'articolo 70, paragrafo 2, di valutare la questione al fine di adottare le misure di controllo ed esecuzione necessarie per garantire la tempestiva conformità al presente regolamento. Tale richiesta è debitamente motivata e indica almeno:

a) il nome del fornitore o del deployer interessato;

b) una descrizione dei fatti pertinenti, le disposizioni del presente regolamento asseritamente violate ed eventuali motivi fondati e sufficienti per sospettare una violazione, compresa, se del caso, la descrizione degli effetti negativi della presunta violazione;

c) l'autorità di vigilanza del mercato che presenta la richiesta.

L'ufficio per l'IA tiene nella massima considerazione la richiesta e l'autorità di vigilanza del mercato coopera attivamente e presta all'ufficio per l'IA l'assistenza necessaria per l'esercizio dei suoi poteri conformemente al paragrafo 1 bis.

Senza indebito ritardo e in ogni caso entro quattro mesi dal ricevimento della richiesta, l'ufficio per l'IA comunica al punto di contatto unico l'intenzione di esercitare i propri poteri conformemente all'articolo 75 bis oppure i motivi per cui non intende esercitarli. Qualora decida di esercitare i propri poteri conformemente all'articolo 75 bis, l'ufficio per l'IA informa periodicamente tale punto di contatto unico in merito ai principali sviluppi del procedimento e al suo esito, senza divulgare informazioni riservate.

3. Qualora non sia in grado di concludere la propria indagine sul sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali nonostante abbia compiuto tutti gli sforzi opportuni per ottenere tali informazioni, un'autorità di vigilanza del mercato può

presentare una richiesta motivata all'ufficio per l'IA, che garantisce l'accesso a tali informazioni. In tal caso, l'ufficio per l'IA fornisce all'autorità richiedente senza indugio, e in ogni caso entro 30 giorni, tutte le informazioni che esso ritiene pertinenti al fine di stabilire se un sistema di IA ad alto rischio non è conforme. Le autorità di vigilanza del mercato salvaguardano la riservatezza delle informazioni ottenute conformemente all'articolo 78 del presente regolamento. La procedura di cui al capo VI del regolamento (UE) 2019/1020 si applica mutatis mutandis.

ARTICOLO 75-BIS

Poteri di controllo ed esecuzione dell'ufficio per l'IA

1. Nell'esercizio dei suoi compiti di controllo ed esecuzione di cui all'articolo 75, paragrafo 1, del presente regolamento l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato previsti dalla presente sezione nonché dall'articolo 14, paragrafo 4, e dall'articolo 16, paragrafo 3, del regolamento (UE) 2019/1020. L'ufficio per l'IA è autorizzato a recuperare integralmente dall'operatore pertinente la totalità dei costi delle sue attività di controllo ed esecuzione in relazione ai casi di non conformità, inclusi i costi per le risorse umane e tecniche, conformemente all'articolo 15 del regolamento (UE) 2019/1020. L'articolo 17 del regolamento (UE) 2019/1020 si applica mutatis mutandis.

2. Qualora abbia motivi ragionevoli per sospettare la non conformità al presente regolamento da parte di un fornitore o di un deployer di un sistema di IA di cui all'articolo 75, paragrafo 1, del presente regolamento l'ufficio per l'IA può adottare una decisione di avviare un'indagine su tale non conformità conformemente all'articolo 14, paragrafo 4, lettera f), del regolamento (UE) 2019/1020. L'ufficio per l'IA notifica all'operatore del sistema di IA interessato l'avvio di tale indagine. L'ufficio per l'IA può esercitare i poteri di cui al paragrafo 1 del presente articolo di propria iniziativa o a seguito di un reclamo ricevuto a norma dell'articolo 85 del presente regolamento, anche prima di avviare un'indagine a norma dell'articolo 14, paragrafo 4, lettera f), del regolamento (UE) 2019/1020.

Qualora abbia motivo di sospettare la non conformità al presente regolamento da parte di un fornitore o di un deployer di un sistema di IA di cui all'articolo 75, paragrafo 1, l'autorità di vigilanza del mercato può inviare all'ufficio per l'IA una richiesta affinché valuti la questione.

3. L'ufficio per l'IA può esercitare i poteri di cui all'articolo 14, paragrafo 4, lettere a), b) e c), del regolamento (UE) 2019/1020 e all'articolo 74, paragrafi 12 e 13, del presente regolamento mediante richiesta semplice o decisione.

Nel richiedere informazioni, l'ufficio per l'IA indica la base giuridica e la finalità della richiesta, specifica quali informazioni sono richieste e fissa il termine entro il quale le informazioni devono essere fornite. Qualora si tratti di una richiesta semplice, l'ufficio per l'IA precisa inoltre che, sebbene non vi sia alcun obbligo di fornire le informazioni richieste, in caso di risposta volontaria le informazioni devono essere corrette e non fuorvianti e indica le potenziali sanzioni pecuniarie di cui all'articolo 99, paragrafo 5, in caso di fornitura di informazioni inesatte o fuorvianti. Qualora la richiesta sia presentata mediante decisione, l'ufficio per l'IA indica inoltre le sanzioni pecuniarie di cui all'articolo 99, paragrafo 5, in caso di fornitura di informazioni inesatte, incomplete o fuorvianti e indica il diritto di chiedere la revisione della decisione alla Corte di giustizia dell'Unione europea. L'ufficio per l'IA trasmette una copia della richiesta all'autorità di vigilanza del mercato dello Stato membro nel cui territorio è situato l'operatore o il suo rappresentante legale.

4. Al fine di svolgere i compiti ad esso assegnati a norma della presente sezione, l'ufficio per l'IA può effettuare tutte le necessarie ispezioni a distanza o in loco in virtù dei poteri di cui all'articolo 14, paragrafo 4, lettere d) ed e), del regolamento (UE) 2019/1020 e all'articolo 74, paragrafo 5, del presente regolamento. Quando effettua un'ispezione, l'ufficio per l'IA informa il fornitore interessato dell'oggetto e della finalità dell'indagine, delle pertinenti sanzioni pecuniarie di cui all'articolo 99, paragrafo 5, del presente regolamento nonché del diritto di chiedere la revisione della decisione alla Corte di giustizia dell'Unione europea. Prima di effettuare un'ispezione, l'ufficio per l'IA informa l'autorità di vigilanza del mercato dello Stato membro nel cui territorio è situato l'operatore o il suo rappresentante legale.

Nel corso di tale ispezione, al personale dell'ufficio per l'IA è conferito il potere di:

a) accedere a tutti i locali, i terreni o le proprietà aziendali dell'operatore interessato situati nell'Unione;

b) esaminare i registri, i dati e altri materiali rilevanti per l'esecuzione dei loro compiti, su qualsiasi forma di supporto;

c) prendere o ottenere sotto qualsiasi forma copie o estratti di registri, dati e qualsiasi altro documento;

d) chiedere a una qualsiasi delle persone soggette all'ispezione o ai loro rappresentanti, o a membri del personale spiegazioni orali o scritte su fattori o documenti relativi all'oggetto e alle finalità dell'ispezione e registrarne le risposte;

e) apporre sigilli ai locali, ai registri o ai documenti aziendali per la durata dell'ispezione e nella misura necessaria al suo espletamento.

Se l'ufficio per l'IA constata che una persona fisica o giuridica si oppone a un'ispezione o la ostacola, l'autorità nazionale competente dello Stato membro interessato presta la necessaria assistenza, richiedendo, se del caso, l'assistenza della polizia o di un'autorità di contrasto equivalente, affinché possa effettuare l'ispezione in loco.

Se l'ispezione in loco di locali, terreni o proprietà aziendali richiede l'autorizzazione di un'autorità giudiziaria conformemente al diritto nazionale, l'ufficio per l'IA richiede tale autorizzazione. L'ufficio per l'IA può richiedere tale autorizzazione anche in via preventiva. Qualora sia richiesta tale autorizzazione, l'au-

torità giudiziaria nazionale verifica tempestivamente che le misure coercitive previste non siano né arbitrarie né sproporzionate tenuto conto dell'oggetto dell'indagine o dell'ispezione nonché dei documenti forniti dall'ufficio per l'IA unitamente alla decisione. Nel verificare la proporzionalità delle misure coercitive, l'autorità giudiziaria nazionale può chiedere all'ufficio per l'IA di fornire spiegazioni dettagliate, in particolare sui motivi per i quali l'ufficio per l'IA sospetta una violazione del presente regolamento e sulla gravità della violazione sospettata e, se del caso, sulla natura del coinvolgimento della persona soggetta alle misure coercitive. L'autorità giudiziaria nazionale non può mettere in discussione la necessità dell'indagine o dell'ispezione, né esigere informazioni contenute nel fascicolo dell'ufficio per l'IA. Conformemente ai trattati, il controllo della legittimità della decisione dell'ufficio per l'IA compete esclusivamente alla Corte di giustizia dell'Unione europea.

5. Su richiesta dell'ufficio per l'IA, l'autorità di vigilanza del mercato competente di uno Stato membro può svolgere nel proprio territorio qualsiasi indagine, ispezione o porre in essere altra misura di accertamento dei fatti in nome e per conto dell'ufficio per l'IA al fine di stabilire se vi sia stata una violazione del presente regolamento. I funzionari delle autorità competenti degli Stati membri incaricati di procedere a tali indagini, ispezioni o porre in essere misure di accertamento dei fatti, così come le persone da esse autorizzate o nominate, esercitano i loro poteri conformemente al loro diritto nazionale.

6. Oltre ai poteri di cui dispone a norma del paragrafo 1 del presente articolo, l'ufficio per l'IA, nell'esercizio delle sue competenze di cui all'articolo 75, paragrafo 1, può:

a) imporre agli operatori di fornire l'accesso ai loro sistemi di IA e fornire spiegazioni in merito;

b) imporre all'operatore l'obbligo di conservare tutti i dati e i documenti ritenuti necessari per valutare l'attuazione e il rispetto degli obblighi di cui al presente regolamento.

7. Al fine di ricevere assistenza nel monitoraggio dell'effettiva attuazione e della conformità alle pertinenti disposizioni del presente regolamento, così come consulenze o conoscenze specifiche nell'esercizio delle proprie competenze a norma dell'articolo 75, paragrafo 1, l'ufficio per l'IA può nominare esperti e revisori esterni indipendenti, nonché esperti, squadre investigative e revisori delle autorità competenti dello Stato membro, con l'accordo dell'autorità interessata. Le informazioni ottenute a seguito di tali azioni di monitoraggio sono condivise con le pertinenti autorità competenti degli Stati membri.

8. Le informazioni raccolte a norma del presente articolo sono utilizzate esclusivamente ai fini del presente regolamento.

Articolo 75-ter

Impegni

Se, nel corso di un procedimento a norma dell'articolo 75 bis, paragrafo 2, l'operatore interessato offre di assumersi impegni volti a garantire la conformità alle pertinenti disposizioni del presente regolamento, l'ufficio per l'IA può, mediante decisione, rendere tali impegni vincolanti per tale operatore e dichiarare che non vi sono ulteriori motivi di intervento. L'ufficio per l'IA, su richiesta o di propria iniziativa, può riaprire il procedimento qualora:

a) si sia prodotto un cambiamento sostanziale di uno dei fatti su cui si è fondata la decisione;

b) l'operatore agisca in contrasto con i propri impegni; oppure

c) la decisione sia stata fondata su informazioni incomplete, inesatte o fuorvianti trasmesse dall'operatore interessato.

Se ritiene che gli impegni offerti dal fornitore interessato non siano idonei a garantire l'effettiva conformità alle pertinenti disposizioni del presente regolamento, l'ufficio per l'IA respinge tali impegni in una decisione motivata al momento della conclusione del procedimento.

Articolo 75-quater

Non conformità, sanzioni pecuniarie e penalità di mora

1. L'ufficio per l'IA, qualora constati che un operatore che rientra nell'ambito di applicazione dell'articolo 75, paragrafo 1, non rispetta le pertinenti disposizioni del presente regolamento o gli impegni resi vincolanti a norma dell'articolo 75 ter, adotta una decisione che stabilisce tale non conformità.

2. Prima di adottare una decisione a norma del paragrafo 1, l'ufficio per l'IA comunica le sue constatazioni preliminari all'operatore interessato. Nelle constatazioni preliminari l'ufficio per l'IA spiega le misure che intende adottare, o che ritiene che l'operatore interessato debba adottare, al fine di dar seguito in maniera efficace alle constatazioni preliminari.

3. Nella decisione a norma del paragrafo 1 del presente articolo, l'ufficio per l'IA ordina, se del caso, all'operatore interessato di adottare le misure necessarie per garantire la conformità alle pertinenti disposizioni del presente regolamento entro un termine ragionevole ivi specificato e di fornire informazioni sulle misure che l'operatore intende adottare per conformarsi alla decisione. L'operatore interessato fornisce all'ufficio per l'IA una descrizione delle misure adottate per garantire il rispetto della decisione in seguito alla loro attuazione. Prima di chiedere l'adozione di qualsiasi misura, l'ufficio per l'IA può avviare un dialogo strutturato con l'operatore del sistema di IA in questione. Nel corso di tale dialogo, l'operatore può proporre di assumersi impegni conformemente all'articolo 75-ter.

4. Una decisione adottata a norma del paragrafo 1 del presente articolo può essere accompagnata dall'imposizione di sanzioni conformemente all'articolo 99, paragrafi da 3 a 7, le cui disposizioni si applicano mutatis mutandis all'ufficio per l'IA nell'esecuzione dei suoi compiti di controllo ed esecuzione di cui all'articolo 75, paragrafo 1.

In particolare, sono soggetti alle sanzioni amministrative pecuniarie di cui all'articolo 99, paragrafo 4:

a) la violazione di qualsiasi applicabile disposizione del presente regolamento, comprese quelle non elencate all'articolo 99, paragrafo 4;

b) il mancato rispetto delle decisioni o delle misure adottate in virtù dei poteri di cui all'articolo 14, paragrafo 4, o all'articolo 16, paragrafo 3, del regolamento (UE) 2019/1020, nonché dei poteri di cui all'articolo 75 bis del presente regolamento;

c) il mancato rispetto di un impegno reso vincolante da una decisione adottata a norma dell'articolo 75-ter.

La fornitura di informazioni inesatte, incomplete o fuorvianti all'ufficio per l'IA per dare seguito a una richiesta è soggetta alle sanzioni amministrative pecuniarie di cui all'articolo 99, paragrafo 5.

5. L'ufficio per l'IA può adottare una decisione che impone penalità di mora al fine di obbligare gli operatori, per i quali è competente a norma dell'articolo 75, paragrafo 1, a:

a) sottoporsi a un'indagine;

b) a dar seguito a una richiesta di informazioni disposta da una decisione a norma dell'articolo 75-bis, paragrafo 3;

c) sottoporsi a un'ispezione disposta da una decisione a norma dell'articolo 75 bis, paragrafo 4;

d) fornire risposte o spiegazioni corrette e complete nel contesto di un'ispezione disposta da una decisione a norma dell'articolo 75 bis, paragrafo 4;

e) conformarsi alle azioni correttive disposte in virtù dei poteri di cui all'articolo 16 del regolamento (UE) 2019/1020;

f) rispettare gli impegni resi giuridicamente vincolanti mediante decisione a norma dell'articolo 75-ter; oppure

g) conformarsi a una decisione adottata a norma del paragrafo 1 del presente articolo.

Tali penalità di mora sono effettive e proporzionate e, se del caso, il loro importo giornaliero non supera il 5 % del reddito medio giornaliero o del fatturato annuo mondiale dell'esercizio precedente, calcolato a decorrere dalla data stabilita nella decisione.

6. La Corte di giustizia dell'Unione europea ha competenza giurisdizionale anche di merito per esaminare le decisioni dell'ufficio per l'IA che fissano una sanzione pecuniaria o una penalità di mora a norma del presente articolo. Essa può estinguere, ridurre o aumentare la sanzione pecuniaria o la penalità di mora inflitta.

7. I fondi raccolti mediante l'imposizione di sanzioni pecuniarie o penalità di mora a norma del presente articolo contribuiscono al bilancio generale dell'Unione.

8. I poteri conferiti all'ufficio per l'IA dal presente articolo sono soggetti a un termine di prescrizione di cinque anni. Il termine di prescrizione decorre dal giorno in cui è stata commessa la violazione. Nel caso di violazioni continuate o ripetute il termine di prescrizione decorre invece dal giorno in cui è cessata la violazione.

Il potere dell'ufficio per l'IA di dare esecuzione delle decisioni adottate ai sensi del presente articolo è soggetto a un termine di prescrizione di cinque anni. Il termine di prescrizione decorre dal giorno in cui la decisione diventa definitiva.

L'atto di esecuzione di cui all'articolo 75 quinquies, paragrafo 3, specifica il primo e il secondo comma del presente paragrafo, nonché le circostanze in cui i termini di prescrizione sono interrotti.

9. Qualora accerti l'assenza di motivi per adottare una decisione di non conformità, l'ufficio per l'IA chiude il procedimento mediante una decisione. Tale decisione si applica con effetto immediato.

ARTICOLO 75-QUINQUIES
Garanzie e ulteriori precisazioni

1. L'articolo 18 del regolamento (UE) 2019/1020 si applica mutatis mutandis agli operatori per i quali l'ufficio per l'IA è competente a norma dell'articolo 75, paragrafo 1 del presente regolamento, fatti salvi i diritti procedurali più specifici previsti dal presente regolamento.

2. Nel corso del procedimento sono pienamente garantiti i diritti di difesa e di accesso al fascicolo degli operatori che rientrano nell'ambito di applicazione dell'articolo 75, paragrafo 1. In considerazione dell'eventuale adozione di decisioni sulla base dell'articolo 75 quater, paragrafo 1, tali operatori hanno il diritto di accedere al fascicolo dell'ufficio per l'IA nel rispetto della procedura di divulgazione negoziata, fermo restando l'interesse legittimo dell'operatore o di un'altra persona interessata alla tutela dei propri segreti aziendali. L'ufficio per l'IA ha il potere di adottare decisioni che stabiliscono tale procedura di divulgazione in caso di disaccordo tra le parti. Il diritto di accesso al fascicolo non si estende alle informazioni riservate e ai documenti interni dell'ufficio per l'IA, del consiglio per l'IA, delle autorità di vigilanza del mercato competenti o di altre autorità pubbliche degli Stati membri. In particolare, il diritto di accesso non si estende alla corrispondenza fra l'ufficio per l'IA e tali autorità. Nessuna disposizione del presente paragrafo osta a che l'ufficio per l'IA divulghi e utilizzi le informazioni necessarie a dimostrare l'esistenza di una violazione.

3. La Commissione può adottare atti di esecuzione riguardanti le modalità pratiche per l'accesso al fascicolo e la divulgazione negoziata delle informazioni di cui al paragrafo 2.

4. L'ufficio per l'IA pubblica le decisioni adottate a norma degli articoli 75 ter e 75 quater. Tale pubblicazione indica i nomi delle parti e il contenuto essenziale della decisione, comprese eventuali sanzioni irrogate. La pubblicazione tiene conto del diritto e dell'interesse legittimo di qualsiasi persona interessata alla protezione delle proprie informazioni riservate.

ARTICOLO 76
Controllo delle prove in condizioni reali da parte delle autorità di vigilanza del mercato

1. Le autorità di vigilanza del mercato hanno le competenze e i poteri per garantire che le prove in condizioni reali siano conformi al presente regolamento.

Qualora le prove in condizioni reali siano fondate sull'articolo 60 bis, qualsiasi riferimento a un'autorità di vigilanza del mercato contenuto nel presente articolo si intende fatto all'autorità nazionale competente o all'autorità appropriata ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, e i riferimenti all'articolo 60 si intendono fatti, se del caso, all'articolo 60 bis.

2. Qualora siano effettuate prove in condizioni reali per i sistemi di IA sottoposti a controllo all'interno di uno spazio di sperimentazione normativa per l'IA a norma dell'articolo 58, le autorità di vigilanza del mercato verificano la conformità dell'articolo 60 nell'ambito del loro ruolo di controllo per lo spazio di sperimentazione normativa per l'IA. Tali autorità possono, se del caso, consentire che le prove in condizioni reali siano effettuate dal fornitore o potenziale fornitore in deroga alle condizioni di cui all'articolo 60, paragrafo 4, lettere f) e g).

3. Qualora sia stata informata dal potenziale fornitore, dal fornitore o da un terzo di un incidente grave o abbia altri motivi per ritenere che le condizioni di cui agli articoli 60 e 61 non siano soddisfatte, un'autorità di vigilanza del mercato può adottare una delle seguenti decisioni sul suo territorio, a seconda dei casi:

a) sospendere o cessare le prove in condizioni reali;

b) imporre al fornitore o potenziale fornitore e al deployer o al potenziale deployer di modificare qualsiasi aspetto delle prove in condizioni reali.

4. Ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3 o sollevato un'obiezione ai sensi dell'articolo 60, paragrafo 4, lettera b), la decisione o l'obiezione ne indica i motivi ed espone le modalità con cui il fornitore o potenziale fornitore può contestare la decisione o l'obiezione.

5. Se del caso, ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3, ne comunica i motivi alle autorità di vigilanza del mercato degli altri Stati membri in cui il sistema di IA è stato sottoposto a prova conformemente al piano di prova.

ARTICOLO 77

Poteri delle autorità che tutelano i diritti fondamentali e cooperazione con le autorità di vigilanza del mercato

1. Le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, hanno il potere di richiedere qualsiasi informazione o documentazione creata o mantenuta dall'autorità di vigilanza del mercato competente a norma del presente regolamento o di accedervi, per via elettronica, in una lingua e in un formato leggibile meccanicamente accessibili, quando l'accesso a tali informazioni o documentazione è necessario per l'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione. Il presente articolo non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti nell'ambito dei loro mandati.

1-bis. Fatte salve le condizioni specificate nel presente articolo, l'autorità di vigilanza del mercato concede all'autorità pubblica o all'organismo pubblico competenti di cui al paragrafo 1 l'accesso a tali informazioni o documentazione, anche richiedendole al fornitore o al deployer, ove necessario e senza indebito ritardo.

1-ter. Le autorità di vigilanza del mercato e le autorità o gli organismi pubblici di cui al paragrafo 1 cooperano strettamente e si prestano reciprocamente l'assistenza necessaria per l'adempimento dei rispettivi mandati, al fine di garantire l'applicazione coerente del presente regolamento e del diritto dell'Unione a tutela dei diritti fondamentali e di razionalizzare le procedure, rispettando nel contempo i rispettivi compiti, competenze, poteri e indipendenza. Ciò include, in particolare, lo scambio di informazioni, ove necessario, per l'efficace supervisione o esecuzione del presente regolamento e delle altre rispettive normative dell'Unione.

2. Entro il 2 novembre 2024 ciascuno Stato membro individua le autorità o gli organismi pubblici di cui al paragrafo 1 e ne pubblica l'elenco. Gli Stati membri notificano l'elenco alla Commissione e agli altri Stati membri e lo tengono aggiornato.

3. Qualora la documentazione di cui al paragrafo 1 non sia sufficiente per accertare un'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità pubblica o l'organismo pubblico di cui al paragrafo 1 può presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici. L'autorità di vigilanza del mercato organizza le prove coinvolgendo da vicino l'autorità pubblica o l'organismo pubblico richiedente entro un termine ragionevole dalla richiesta.

4. Qualsiasi informazione o documentazione ottenuta a norma del presente articolo dalle autorità o dagli organismi pubblici nazionali di cui al paragrafo 1 del presente articolo è trattata in conformità degli obblighi di riservatezza stabiliti all'articolo 78.

ARTICOLO 78

Riservatezza

omissis

ARTICOLO 79

Procedura a livello nazionale per i sistemi di IA che presentano un rischio

omissis

ARTICOLO 80

Procedura per i sistemi di IA classificati dal fornitore come non ad alto rischio in applicazione dell'allegato III

omissis

ARTICOLO 81

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di

cui all'articolo 79, paragrafo 5, o entro 30 giorni in caso omissis

ARTICOLO 82
Sistemi di IA conformi che presentano un rischio
omissis

ARTICOLO 83
Non conformità formale
omissis

ARTICOLO 84
Strutture di sostegno dell'Unione per la prova dell'IA
omissis

SEZIONE 4
Mezzi di ricorso

ARTICOLO 85
Diritto di presentare un reclamo a un'autorità di vigilanza del mercato
omissis

ARTICOLO 86
Diritto alla spiegazione dei singoli processi decisionali
omissis

ARTICOLO 87
Segnalazione delle violazioni e protezione delle persone segnalanti
omissis

SEZIONE 5
Supervisione, indagini, esecuzione e monitoraggio in relazione ai fornitori di modelli di IA per finalità generali

ARTICOLO 88
Esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali
omissis

ARTICOLO 89
Azioni di monitoraggio
omissis

ARTICOLO 90
Segnalazioni di rischi sistemici da parte del gruppo di esperti scientifici
omissis

ARTICOLO 91
Potere di richiedere documentazione e informazioni
omissis

ARTICOLO 92
Potere di effettuare valutazioni
omissis

ARTICOLO 93
Potere di richiedere misure
omissis

ARTICOLO 94
Diritti procedurali degli operatori economici del modello di IA per finalità generali
omissis

CAPO X
CODICI DI CONDOTTA E ORIENTAMENTI

ARTICOLO 95
Codici di condotta per l'applicazione volontaria di requisiti specifici

1. L'ufficio per l'IA e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta, compresi i relativi meccanismi di governance, intesi a promuovere l'applicazione volontaria ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti di cui al capo III, sezione 2, tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore che consentono l'applicazione di tali requisiti.

2. L'ufficio per l'IA e gli Stati membri agevolano l'elaborazione di codici di condotta relativi all'applicazione volontaria, anche da parte dei deployer, di requisiti specifici a tutti i sistemi di IA, sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi, compresi elementi quali, a titolo puramente esemplificativo:

a) gli elementi applicabili previsti negli orientamenti etici dell'Unione per un'IA affidabile;

b) la valutazione e la riduzione al minimo dell'impatto dei sistemi di IA sulla sostenibilità ambientale, anche per quanto riguarda la programmazione efficiente sotto il profilo energetico e le tecniche per la progettazione, l'addestramento e l'uso efficienti dell'IA;

c) la promozione dell'alfabetizzazione in materia di IA, in particolare quella delle persone che si occupano dello sviluppo, del funzionamento e dell'uso dell'IA;

d) la facilitazione di una progettazione inclusiva e diversificata dei sistemi di IA, anche attraverso la creazione di gruppi di sviluppo inclusivi e diversificati e la promozione della partecipazione dei portatori di interessi a tale processo;

e) la valutazione e la prevenzione dell'impatto negativo dei sistemi di IA sulle persone vulnerabili o sui gruppi di persone vulnerabili, anche per quanto riguarda l'accessibilità per le persone con disabilità, nonché sulla parità di genere.

3. I codici di condotta possono essere elaborati da singoli fornitori o deployer di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione di qualsiasi portatore di interessi e delle sue organizzazioni rappresentative, comprese le organizzazioni della società civile e il mondo accademico. I codici di condotta possono riguardare uno o più sistemi di IA tenendo conto della similarità della finalità prevista dei sistemi pertinenti.

4. Nell'incoraggiare e agevolare l'elaborazione dei codici di condotta, l'ufficio per l'IA e gli Stati membri tengono conto degli interessi e delle esigenze specifici delle PMI, comprese le start-up, e delle piccole imprese a media capitalizzazione.

ARTICOLO 96
Orientamenti della Commissione sull'attuazione del regolamento

1. La Commissione elabora orientamenti sull'attua-

zione pratica del presente regolamento, in particolare per quanto riguarda:

a) l'applicazione dei requisiti e degli obblighi di cui agli articoli da 8 a 15 e agli articoli 25 e 26;

b) le pratiche vietate di cui all'articolo 5;

c) l'attuazione pratica delle disposizioni relative alla modifica sostanziale;

d) l'attuazione pratica degli obblighi di trasparenza di cui all'articolo 50;

e) informazioni dettagliate sulla relazione del presente regolamento con la normativa di armonizzazione dell'Unione elencata nell'allegato I, nonché con altre disposizioni pertinenti di diritto dell'Unione, anche per quanto riguarda la coerenza nella loro applicazione;

f) l'applicazione della definizione di sistema di IA di cui all'articolo 3, punto 1);

g) l'attuazione pratica dell'articolo 8, paragrafo 2, dell'articolo 9, paragrafo 10, e dell'articolo 17, paragrafo 3, conformemente al principio di complementarità e proporzionalità, al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi per la conformità ai requisiti del presente regolamento e ai requisiti della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A; tali orientamenti sono pubblicati entro il 1° agosto 2027.

Quando pubblica tali orientamenti, la Commissione coinvolge il consiglio per l'IA e presta particolare attenzione alle esigenze delle PMI, comprese le start-up, e delle piccole imprese a media capitalizzazione, delle autorità pubbliche locali e dei settori maggiormente interessati dal presente regolamento.

Gli orientamenti di cui al primo comma del presente paragrafo tengono debitamente conto dello stato dell'arte generalmente riconosciuto in materia di IA, nonché delle pertinenti norme armonizzate e specifiche comuni di cui agli articoli 40 e 41, o delle norme armonizzate o specifiche tecniche stabilite a norma della normativa di armonizzazione dell'Unione.

2. Su richiesta degli Stati membri o dell'ufficio per l'IA, o di propria iniziativa, la Commissione aggiorna gli orientamenti adottati quando lo ritiene necessario.

CAPO XI
DELEGA DI POTERE E PROCEDURA DI COMITATO

ARTICOLO 97
Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 1o agosto 2024. Il potere di adottare atti delegati di cui all'articolo 2, paragrafo 13, e all'articolo 30, paragrafo 2, è conferito alla Commissione per un periodo di cinque anni a decorrere dal 27 luglio 2026. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 2, paragrafo 13, all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 30, paragrafo 2, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale «Legiferare meglio» del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. Qualsiasi atto delegato adottato a norma dell'articolo 2, paragrafo 13, dell'articolo 6, paragrafi 6 o 7, dell'articolo 7, paragrafi 1 o 3, dell'articolo 11, paragrafo 3, dell'articolo 30, paragrafo 2, dell'articolo 43, paragrafi 5 o 6, dell'articolo 47, paragrafo 5, dell'articolo 51, paragrafo 3, dell'articolo 52, paragrafo 4, o dell'articolo 53, paragrafi 5 o 6, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

ARTICOLO 98
Procedura di comitato

omissis

CAPO XII
SANZIONI

ARTICOLO 99
Sanzioni

1. In conformità dei termini e delle condizioni di cui al presente regolamento, gli Stati membri stabiliscono le norme relative alle sanzioni e alle altre misure di esecuzione, che possono includere anche sanzioni amministrative pecuniarie, avvertimenti e misure non pecuniarie, applicabili a qualsiasi violazione del presente

regolamento da parte degli operatori, e adottano tutte le misure necessarie per garantirne un'attuazione corretta ed efficace, tenendo conto degli orientamenti emanati dalla Commissione a norma dell'articolo 96. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Nell'imporre le sanzioni, gli Stati membri tengono conto degli interessi delle PMI, comprese le start-up, e delle piccole imprese a media capitalizzazione, e della loro sostenibilità economica.

2. Gli Stati membri notificano alla Commissione, senza indugio e al più tardi entro la data di entrata in applicazione, le norme relative alle sanzioni e le altre misure di esecuzione di cui al paragrafo 1, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.

3. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35 000 000 EUR o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. La non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi dei fornitori a norma dell'articolo 16;

b) gli obblighi dei rappresentati autorizzati a norma dell'articolo 22;

c) gli obblighi degli importatori a norma dell'articolo 23;

d) gli obblighi dei distributori a norma dell'articolo 24;

d-bis) gli obblighi dei fornitori e degli operatori a norma dell'articolo 25, paragrafi 2 e 4;

e) gli obblighi dei deployer a norma dell'articolo 26;

f) i requisiti e gli obblighi degli organismi notificati a norma dell'articolo 31, dell'articolo 33, paragrafi 1, 3 e 4, o dell'articolo 34;

g) gli obblighi di trasparenza per i fornitori e i deployers a norma dell'articolo 50.

5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 7 500 000 EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

6. Nel caso delle PMI, comprese le start-up, ciascuna sanzione pecuniaria di cui al presente articolo è pari al massimo alle percentuali o all'importo di cui ai paragrafi 3, 4 e 5, se inferiore.

6 bis. Nel caso delle piccole imprese a media capitalizzazione, ciascuna sanzione pecuniaria di cui ai paragrafi 4 e 5 è pari al massimo alle percentuali o all'importo di cui a tali paragrafi, se inferiore.

7. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e, se del caso, si tiene in considerazione quanto segue:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA, nonché, ove opportuno, il numero di persone interessate e il livello del danno da esse subito;

b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione;

c) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento;

d) le dimensioni, il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione;

e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione;

f) il grado di cooperazione con le autorità nazionali competenti al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) il grado di responsabilità dell'operatore tenendo conto delle misure tecniche e organizzative attuate;

h) il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore;

i) il carattere doloso o colposo della violazione;

j) l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate.

8. Ciascuno Stato membro può prevedere norme che dispongano in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

9. A seconda dell'ordinamento giuridico degli Stati membri, le norme in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che le sanzioni pecuniarie siano inflitte dalle autorità giudiziarie nazionali competenti o da altri organismi, quali applicabili in tali Stati membri. L'applicazione di tali norme in tali Stati membri ha effetto equivalente.

10. L'esercizio dei poteri attribuiti dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

11. Gli Stati membri riferiscono annualmente alla Commissione in merito alle sanzioni amministrative pecuniarie inflitte nel corso dell'anno, in conformità del presente articolo, e a eventuali controversie o procedimenti giudiziari correlati.

ARTICOLO 100

Sanzioni amministrative pecuniarie inflitte a istituzioni, organi e organismi dell'Unione

omissis

ARTICOLO 101

Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali

omissis

CAPO XIII
DISPOSIZIONI FINALI

ARTICOLO 102

Modifica del regolamento (CE) n. 300/2008

omissis

ARTICOLO 103

Modifica del regolamento (UE) n. 167/2013

omissis

ARTICOLO 104

Modifica del regolamento (UE) n. 168/2013

omissis

ARTICOLO 105

Modifica della direttiva 2014/90/UE

omissis

ARTICOLO 106

Modifica della direttiva (UE) 2016/797

omissis

ARTICOLO 107

Modifica del regolamento (UE) 2018/858

omissis

ARTICOLO 108

Modifiche del regolamento (UE) 2018/1139

omissis

ARTICOLO 109

Modifica del regolamento (UE) 2019/2144

omissis

ARTICOLO 110

Modifica della direttiva (UE) 2020/1828

omissis

ARTICOLO 111

Sistemi di IA già immessi sul mercato o messi in servizio e modelli di IA per finalità generali già immessi sul mercato

1. Fatta salva l'applicazione dell'articolo 5 di cui all'articolo 113, paragrafo 3, lettera a), i sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato X che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2027 sono resi conformi al presente regolamento entro il 31 dicembre 2030.

Si tiene conto dei requisiti di cui al presente regolamento nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato X da effettuare come previsto in tali atti giuridici e ove tali atti giuridici siano sostituiti o modificati.

2. Fatta salva l'applicazione dell'articolo 5, di cui all'articolo 113, terzo comma, lettera a), il presente regolamento si applica agli operatori dei sistemi di IA ad alto rischio, diversi dai sistemi di cui al paragrafo 1 del presente articolo, che sono stati immessi sul mercato o messi in servizio prima della data di applicazione del capo III di cui all'articolo 113 solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione. In ogni caso, i fornitori e deployer di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche adottano le misure necessarie per conformarsi ai requisiti e agli obblighi di cui al presente regolamento entro il 2 agosto 2030.

3. I fornitori di modelli di IA per finalità generali che sono stati immessi sul mercato prima del 2 agosto 2025 adottano le misure necessarie per conformarsi agli obblighi di cui al presente regolamento entro 2 agosto 2027.

4. I fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, immessi sul mercato prima del 2 agosto 2026, adottano le misure necessarie per conformarsi all'articolo 50, paragrafo 2, entro il 2 dicembre 2026.

ARTICOLO 112

Valutazione e riesame

omissis

ARTICOLO 113

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

Si applica a decorrere dal 2 agosto 2026.

Tuttavia:

a) I capi I e II si applicano a decorrere dal 2 febbraio 2025, ad eccezione dell'articolo 5, paragrafo 1, primo comma, lettere b-bis) e b-ter), e dell'articolo 5, paragrafi 1 bis e 1 ter, che si applicano a decorrere dal 2 dicembre 2026;

b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal 2 agosto 2025, ad eccezione dell'articolo 101;

c) Il capo III, sezioni 1, 2 e 3, ad eccezione dell'articolo 6, paragrafo 5, si applica a decorrere dal:

i) 2 dicembre 2027 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III; e

ii) 2 agosto 2028 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, e dell'allegato I;

d) Gli articoli da 102 a 110 si applicano a decorrere dal 27 luglio 2026.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

ALLEGATO I

Elenco della normativa di armonizzazione dell'Unione

Sezione A. Elenco della normativa di armonizzazione dell'Unione in base al nuovo quadro legislativo

1. Soppresso

2. direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli (GU L 170 del 30.6.2009, pag. 1);

3. direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarca-

zioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE (GU L 354 del 28.12.2013, pag. 90);

4. direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori (GU L 96 del 29.3.2014, pag. 251);

5. direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva (GU L 96 del 29.3.2014, pag. 309);

6. direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62);

7. direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione (GU L 189 del 27.6.2014, pag. 164);

8. regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la direttiva 2000/9/CE (GU L 81 del 31.3.2016, pag. 1);

9. regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio (GU L 81 del 31.3.2016, pag. 51);

10. regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE (GU L 81 del 31.3.2016, pag. 99);

11. regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1);

12. regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

Sezione B – Elenco di altre normative di armonizzazione dell'Unione

13. Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72);

14. regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli (GU L 60 del 2.3.2013, pag. 52);

15. regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1);

16. direttiva 2014/90/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'equipaggiamento marittimo e che abroga la direttiva 96/98/CE del Consiglio (GU L 257 del 28.8.2014, pag. 146);

17. direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea (GU L 138 del 26.5.2016, pag. 44);

18. regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (GU L 151 del 14.6.2018, pag. 1);

19. regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010, (UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011,(UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012,(UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione (GU L 325 del 16.12.2019, pag. 1);

20. regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1), nella misura in cui si tratta della progettazione, della produzione e dell'immissione sul mercato degli aeromobili di cui all'articolo 2, paragrafo 1, lettere a) e b), relativamente agli aeromobili senza equipaggio e ai loro motori, eliche, parti e dispositivi di controllo remoto;

21. regolamento (UE) 2023/1230 del Parlamento europeo e del Consiglio, del 14 giugno 2023, relativo alle macchine e che abroga la direttiva 2006/42/CE del Parlamento europeo e del Consiglio e la direttiva 73/361/CEE del Consiglio (GU L 165 del 29.6.2023, pag. 1, ELI: http://data.europa.eu/eli/reg/2023/1230/oj).

ALLEGATO II

Elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii)

omissis

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

omissis

ALLEGATO IV

Documentazione tecnica di cui all'articolo 11, paragrafo 1

omissis

ALLEGATO V

Dichiarazione di conformità UE

omissis

ALLEGATO VI

Procedura di valutazione della conformità basata sul controllo interno

omissis

ALLEGATO VII

Conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica

omissis

ALLEGATO VIII

Informazioni da presentare all'atto della registrazione di sistemi di IA ad alto rischio in conformità dell'articolo 49

Sezione A - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 1

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49, paragrafo 1:

1. il nome, l'indirizzo e i dati di contatto del fornitore;

2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;

3.il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;

4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;

5. la descrizione della finalità prevista del sistema di IA e dei componenti e delle funzioni supportati da tale sistema di IA;

6. una descrizione di base concisa delle informazioni utilizzate dal sistema (dati, input) e della sua logica operativa;

7. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato);

8. il tipo, il numero e la data di scadenza del certificato rilasciato dall'organismo notificato e il nome o il numero di identificazione di tale organismo notificato, ove applicabile;

9. una copia scannerizzata del certificato di cui al punto 8, ove applicabile;

10. eventuali Stati membri dell'Unione in cui il sistema di IA è stato immesso sul mercato, messo in servizio o reso disponibile;

11. una copia della dichiarazione di conformità UE di cui all'articolo 47;

12. le istruzioni per l'uso in formato elettronico; questa informazione non deve essere fornita per i sistemi di IA ad alto rischio nei settori delle attività di contrasto o della migrazione, dell'asilo e della gestione del controllo delle frontiere di cui all'allegato III, punti 1, 6 e 7;

13. un indirizzo internet per ulteriori informazioni (facoltativo).

Sezione B - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 2

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA che devono essere registrati a norma dell'articolo 49, paragrafo 2:

1.il nome, l'indirizzo e i dati di contatto del fornitore;

2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;

3. il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;

4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;

5. la descrizione della finalità prevista del sistema di IA;

6. la o le condizioni di cui all'articolo 6, paragrafo 3, sulla base delle quali il sistema di IA non è ritenuto ad alto rischio;

7. soppresso

8. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato).

9. soppresso

Sezione C - Informazioni che i deployer di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 3

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49:

1. il nome, l'indirizzo e i dati di contatto del deployer;

2. il nome, l'indirizzo e i dati di contatto della persona che fornisce informazioni a nome del deployer;

3. l'indirizzo internet dell'inserimento del sistema di IA nella banca dati dell'UE da parte del suo fornitore;

4. una sintesi dei risultati della valutazione d'impatto sui diritti fondamentali effettuata a norma dell'articolo 27;

5. una sintesi della valutazione d'impatto sulla protezione dei dati effettuata ai sensi dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, come specificato all'articolo 26, pa-

ragrafo 8, del presente regolamento, ove applicabile.

ALLEGATO IX

Informazioni da presentare all'atto della registrazione dei sistemi di IA ad alto rischio elencati nell'allegato III in relazione alle prove in condizioni reali in conformità dell'articolo 60

omissis

ALLEGATO X

Atti legislativi dell'Unione sui sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

omissis

ALLEGATO XI

Documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a) — documentazione tecnica per i fornitori di modelli di IA per finalità generali

omissis

ALLEGATO XII

Informazioni sulla trasparenza di cui all'articolo 53, paragrafo 1, lettera b) - documentazione tecnica per i fornitori di modelli di IA per finalità generali ai fornitori a valle che integrano il modello nel loro sistema di IA

omissis

ALLEGATO XIII

Criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico di cui all'articolo 51

omissis

ALLEGATO XIV

Elenco dei codici, delle categorie e dei corrispondenti tipi di sistemi di IA ai fini della procedura di notifica di cui all'articolo 30, che specifica l'ambito di applicazione della designazione degli organismi notificati

1. Introduzione

La valutazione della conformità dei sistemi di IA ad alto rischio a norma del presente regolamento può richiedere il coinvolgimento di organismi di valutazione della conformità. Solo gli organismi di valutazione della conformità designati conformemente al presente regolamento possono effettuare valutazioni della conformità e solo per le attività relative ai tipi di sistemi di IA interessati. L'elenco dei codici, delle categorie e dei corrispondenti tipi di sistemi di IA definisce l'ambito di applicazione della designazione degli organismi di valutazione della conformità notificati a norma dell'articolo 30.

2. Elenco dei codici, delle categorie e dei corrispondenti sistemi di IA

a) ***Sistemi di IA soggetti all'allegato I***

Codice AIA	
AIP 0102	**Sistemi di IA soggetti all'allegato I, sezione A, punto 2**
AIP 0103	**Sistemi di IA soggetti all'allegato I, sezione A, punto 3**
AIP 0104	**Sistemi di IA soggetti all'allegato I, sezione A, punto 4**
AIP 0105	**Sistemi di IA soggetti all'allegato I, sezione A, punto 5**
AIP 0106	**Sistemi di IA soggetti all'allegato I, sezione A, punto 6**
AIP 0107	**Sistemi di IA soggetti all'allegato I, sezione A, punto 7**
AIP 0108	**Sistemi di IA soggetti all'allegato I, sezione A, punto 8**
AIP 0109	**Sistemi di IA soggetti all'allegato I, sezione A, punto 9**
AIP 0110	**Sistemi di IA soggetti all'allegato I, sezione A, punto 10**
AIP 0111	**Sistemi di IA soggetti all'allegato I, sezione A, punto 11**
AIP 0112	**Sistemi di IA soggetti all'allegato I, sezione A, punto 12**

b) Sistemi di IA soggetti all'allegato III, punto 1

Codice AIA	
AIB 0201	**Sistemi di identificazione biometrica remota.**
AIB 0202	**Sistemi di IA di categorizzazione biometrica.**
AIB 0203	**Sistemi di IA di riconoscimento delle emozioni.**

3. Codici specifici per la tecnologia di IA

a) IA simbolica e sistemi esperti

Codice AIA	
AIH 0101	**Sistemi di IA basati sull'IA simbolica, sistemi esperti e basati sulla conoscenza e sistemi di IA basati sulla ricerca e sull'ottimizzazione.**

b) Apprendimento automatico, esclusa l'IA generativa e l'IA per finalità generali

Codice AIA	
AIH 0201	**Sistemi di IA che trattano dati strutturati.**
AIH 0202	**Sistemi di IA che trattano dati audio e di segnale.**
AIH 0203	**Sistemi di IA che trattano dati testuali.**

AIH 0204	**Sistemi di IA che trattano immagini e video.**
AIH 0205	**Sistemi di IA che apprendono dal loro ambiente, esclusi i sistemi di IA di cui al codice AIH 0401.**

c) Sistemi di IA basati sull'IA per finalità generali e sull'IA generativa

Codice AIA	
AIH 0301	**Sistemi di IA generativa, compresi i sistemi di IA basati su modelli di IA per finalità generali.**

d) Tecnologie di IA emergenti

Codice AIA	
AIH 0401	**Sistemi di IA basati su altre tecnologie di IA emergenti non contemplate da altri codici, compresa l'IA agentica.**

Domanda di designazione

Gli organismi di valutazione della conformità utilizzano gli elenchi di codici, categorie e corrispondenti tipi di sistemi di IA riportati nel presente allegato quando specificano i tipi di sistemi di IA nella domanda di designazione di cui all'articolo 29.