

# Artificial intelligence act tutte le norme coinvolte

## CAPO I Disposizioni generali

### 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 di-

sposizione 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 del 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) «marcatore 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 di raccogliere 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 per soddisfare determinati requisiti stabiliti 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 del sistema 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 gennaio 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 da 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.

## 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 ingannevoli 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 IA per 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 contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

i) la ricerca mirata di specifiche vittime 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) la localizzazione 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, ogni uso 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 o da 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 autorità 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.

## SEZIONE 2

### Requisiti per i sistemi di IA ad alto rischio

#### ARTICOLO 9

##### *Sistema di gestione dei rischi*

1. In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi.

2. Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso comprende le fasi seguenti:

a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista;

b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile;

c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72;

d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a).

3. I rischi di cui al presente articolo riguardano solo quelli che possono essere ragionevolmente attenuati o eliminati attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate.

4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), tengono in debita considerazione gli effetti e la possibile interazione derivanti dall'applicazione combinata dei requisiti di cui alla presente sezione, al fine di ridurre al minimo i rischi con maggiore efficacia e raggiungere nel contempo un equilibrio adeguato nell'attuazione delle misure volte a soddisfare tali requisiti.

5. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili.

Nell'individuare le misure di gestione dei rischi più appropriate, occorre garantire quanto segue:

a) l'eliminazione o la riduzione dei rischi individuati e valutati a norma del paragrafo 2, per quanto possibile dal punto di vista tecnico attraverso un'adeguata progettazione e fabbricazione del sistema di IA ad alto rischio;

b) ove opportuno, l'attuazione di adeguate misure di attenuazione e di controllo nell'affrontare i rischi che non possono essere eliminati;

c) la fornitura delle informazioni richieste a norma dell'articolo 13 e, ove opportuno, la formazione dei deployer.

Al fine di eliminare o ridurre i rischi connessi all'uso del sistema di IA ad alto rischio, si tengono debitamente in considerazione le conoscenze tecniche, l'esperienza, l'istruzione e la formazione che ci si può aspettare dal deployer e il contesto presumibile in cui il sistema è destinato ad essere usato.

6. I sistemi di IA ad alto rischio sono sottoposti a prova al fine di individuare le misure di gestione dei rischi più appropriate e mirate. Le prove garantiscono che i sistemi di IA ad alto rischio funzionino in modo coerente per la finalità prevista e che siano conformi ai requisiti di cui alla presente sezione.

7. Le procedure di prova possono comprendere prove in condizioni reali conformemente all'articolo 60.

8. Le prove dei sistemi di IA ad alto rischio sono effettuate, a seconda dei casi, in un qualsiasi momento dell'intero processo di sviluppo e, in ogni caso, prima della loro immissione sul mercato o messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite precedentemente e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio.

9. Nell'attuare il sistema di gestione dei rischi di cui

ai paragrafi da 1 a 7, i fornitori prestano attenzione, nell'ottica della sua finalità prevista, all'eventualità che il sistema di IA ad alto rischio possa avere un impatto negativo sulle persone di età inferiore a 18 anni o, a seconda dei casi, su altri gruppi vulnerabili.

10. Per i fornitori di sistemi di IA ad alto rischio soggetti ai requisiti relativi ai processi interni di gestione dei rischi a norma di altre disposizioni pertinenti del diritto dell'Unione, gli aspetti di cui ai paragrafi da 1 a 9 possono far parte delle procedure di gestione dei rischi stabilite a norma di tale diritto oppure essere combinati con le stesse.

#### 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, ogniquale volta 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. Nella misura in cui ciò sia strettamente necessario al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio in conformità del paragrafo 2, lettere f) e g), del presente articolo, 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 devono essere 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 devono essere 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;

f) 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 in-

formazioni 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*

1. I sistemi di IA ad alto rischio consentono a livello tecnico la registrazione automatica degli eventi («log») per la durata del ciclo di vita del sistema.

2. Al fine di garantire un livello di tracciabilità del funzionamento del sistema di IA ad alto rischio adeguato alla finalità prevista del sistema, le capacità di registrazione consentono la registrazione di eventi pertinenti per:

a) l'individuazione di situazioni che possono far sì che il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, o determinare una modifica sostanziale;

b) l'agevolazione del monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; e

c) il monitoraggio del funzionamento dei sistemi di IA ad alto rischio di cui all'articolo 26, paragrafo 5.

3. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le capacità di registrazione comprendono almeno i dati seguenti:

a) la registrazione del periodo di ciascun utilizzo del sistema (data e ora di inizio e di fine di ciascun utilizzo);

b) la banca dati di riferimento utilizzata dal sistema per verificare i dati di input;

c) i dati di input per i quali la ricerca ha portato a una corrispondenza;

d) l'identificativo delle persone fisiche che partecipano alla verifica dei risultati di cui all'articolo 14, paragrafo 5.

## ARTICOLO 14

**Sorveglianza umana**

1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.

2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione.

3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti:

a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile;

b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal deployer.

4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di:

a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese;

b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;

c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;

d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio;

e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.

5. In aggiunta, per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 del presente articolo sono tali da garantire che il deployer non compia azioni o adotti decisioni

sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità.

Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito.

## SEZIONE 3

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

## ARTICOLO 26

**Obblighi dei deployer dei sistemi di IA ad alto rischio**

1. I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 3 e 6.

2. I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.

3. Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale e la libertà del deployer di organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.

4. Fatti salvi i paragrafi 1 e 2, nella misura in cui esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio.

5. I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto.

Per i deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di monitorag-

gio di cui al primo comma si considera soddisfatto se sono soddisfatte le regole sui dispositivi, sui processi e sui meccanismi di governance interna a norma del pertinente diritto in materia di servizi finanziari.

6. I deployer di sistemi di IA ad alto rischio conservano i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

I deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari conservano i log come parte della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

8. I deployer di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione rispettano gli obblighi di registrazione di cui all'articolo 49. Ove accertino che il sistema di IA ad alto rischio che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 71, tali deployer non utilizzano tale sistema e ne informano il fornitore o il distributore.

9. Se del caso, i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 del presente regolamento per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680.

10. Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, ex ante o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.

Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autoriz-

zazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati.

In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa. Occorre garantire che nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota a posteriori.

Il presente paragrafo lascia impregiudicati l'articolo 9 del regolamento (UE) 2016/679 e l'articolo 10 della direttiva (UE) 2016/680 riguardo al trattamento dei dati biometrici.

Indipendentemente dalla finalità o dal deployer, ciascun uso di tali sistemi di IA ad alto rischio è documentato nel pertinente fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Il presente comma lascia impregiudicati i poteri conferiti alle autorità di controllo dalla direttiva (UE) 2016/680.

I deployer presentano alle pertinenti autorità di vigilanza del mercato e alle autorità nazionali per la protezione dei dati relazioni annuali sul loro uso di sistemi di identificazione biometrica remota a posteriori, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Le relazioni possono essere aggregate per coprire più di un utilizzo.

Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota a posteriori.

11. Fatto salvo l'articolo 50, del presente regolamento i deployer dei sistemi di IA ad alto rischio di cui all'allegato III che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche informano queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Per i sistemi di IA ad alto rischio utilizzati a fini di contrasto si applica l'articolo 13 della direttiva (UE) 2016/680.

12. I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad alto rischio ai fini dell'attuazione del presente regolamento.

#### 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.

## CAPO VI Misure a sostegno dell'innovazione

### 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*

1. Nello spazio di sperimentazione normativa per l'IA, i dati personali legalmente raccolti per altre finalità possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando sono soddisfatte tutte le condizioni seguenti:

a) i sistemi di IA sono sviluppati per salvaguardare un interesse pubblico rilevante da parte di un'autorità pubblica o di un'altra persona fisica o giuridica e in uno o più dei settori seguenti:

i) la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari;

ii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la tutela della biodiversità, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi;

iii) la sostenibilità energetica;

iv) la sicurezza e la resilienza dei sistemi di trasporto e della mobilità, delle infrastrutture critiche e delle reti;

v) l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici;

b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al

Capo III, sezione 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali;

c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento;

d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati;

e) i fornitori possono condividere ulteriormente i dati originariamente raccolti solo in conformità del diritto dell'Unione in materia di protezione dei dati; i dati personali creati nello spazio di sperimentazione non possono essere condivisi al di fuori dello spazio di sperimentazione;

f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati né incide sull'applicazione dei loro diritti sanciti dal diritto

dell'Unione in materia di protezione dei dati personali;

g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono protetti mediante adeguate misure tecniche e organizzative e cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali;

h) i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione, salvo diversa disposizione del diritto dell'Unione o nazionale;

i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica di cui all'allegato IV;

j) una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti; tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

2. A fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità di contrasto, il trattamento dei dati personali negli spazi di sperimentazione normativa per l'IA si basa su una specifica disposizione di diritto nazionale o dell'Unione ed è soggetto alle stesse condizioni cumulative di cui al paragrafo 1.

3. Il paragrafo 1 lascia impregiudicate le disposizioni del diritto dell'Unione o nazionale che escludono il trattamento dei dati personali per fini diversi da quelli espressamente menzionati in tali disposizioni, nonché il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali.

## CAPO X

### Codici di condotta e orientamenti

#### ARTICOLO 96

#### *Orientamenti della Commissione sull'attuazione del regolamento*

1. La Commissione elabora orientamenti sull'attuazione 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.

### Allegato 2

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

Reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii):

- terrorismo,
- tratta di esseri umani,
- sfruttamento sessuale di minori e pornografia minorile,
- traffico illecito di stupefacenti o sostanze psicotrope,
- traffico illecito di armi, munizioni ed esplosivi,
- omicidio volontario, lesioni gravi,
- traffico illecito di organi e tessuti umani,
- traffico illecito di materie nucleari e radioattive,
- sequestro, detenzione illegale e presa di ostaggi,
- reati che rientrano nella competenza giurisdizionale della Corte penale internazionale,
- illecita cattura di aeromobile o nave,
- violenza sessuale,
- reato ambientale,
- rapina organizzata o a mano armata,
- sabotaggio,
- partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.

## Allegato 3

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

I sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, sono i sistemi di IA elencati in uno dei settori indicati di seguito.

1. Biometria, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di identificazione biometrica remota.

Non vi rientrano i sistemi di IA destinati a essere utilizzati per la verifica biometrica la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere;

b) i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche;

c) i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni.

2. Infrastrutture critiche: i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità.

3. Istruzione e formazione professionale:

a) i sistemi di IA destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli;

b) i sistemi di IA destinati a essere utilizzati per valutare i risultati dell'apprendimento, anche nei casi in cui tali risultati sono utilizzati per orientare il processo di apprendimento di persone fisiche in istituti di istruzione o formazione professionale a tutti i livelli;

c) i sistemi di IA destinati a essere utilizzati per valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere, nel contesto o all'interno di istituti di istruzione o formazione professionale a tutti i livelli;

d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli.

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;

b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

5. Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi:

a) i sistemi di IA destinati a essere utilizzati dalle au-

torità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;

b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie;

c) i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie;

d) i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza;

6. Attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per determinare il rischio per una persona fisica di diventare vittima di reati;

b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, come poligrafi e strumenti analoghi;

c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;

d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;

e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati.

7. Migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, o da istituzioni, organi e organismi dell'Unione, come poligrafi o strumenti analoghi;

b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;

c) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto o di permesso di soggiorno e per i relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status, compresa le valutazioni correlate dell'affidabilità degli elementi probatori;

d) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, o da istitu-

zioni, organi e organismi dell'Unione, nel contesto della migrazione, dell'asilo o della gestione del controllo delle frontiere, al fine di individuare, riconoscere o identificare persone fisiche, a eccezione della verifica dei documenti di viaggio.

8. Amministrazione della giustizia e processi democratici:

a) i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie;

b) i sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum. Sono esclusi i sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.



**Modulo24**  
**Compliance**

Il Sole  
**24 ORE**  
Professionale

**TUTTO SULLA COMPLIANCE IN**

**UNA PIATTAFORMA DIGITALE EVOLUTA**

Un servizio di aggiornamento tempestivo sulle novità normative e giurisprudenziali dedicate a ESG, Data Protection e GDPR, Whistleblowing e 231 grazie alle news quotidiane, le rassegne di giurisprudenza, gli approfondimenti d'autore integrati a strumenti utili per l'azienda e il legale.



**SCOPRI DI PIÙ**  
**modulo24compliance.com**

Gruppo Il Sole  
**24 ORE**