Consiglio dell'Unione europea

Bruxelles, 6 dicembre 2022
(OR. en)

15698/22

Fascicolo interistituzionale: 2021/0106(COD)

TELECOM 516
JAI 1633
COPEN 434
CYBER 399
DATAPROTECT 351
EJUSTICE 95
COSI 318
IXIM 291
ENFOPOL 626
RELEX 1674
MI 918
COMPET 1005
CODEC 1940

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	6 dicembre 2022
Destinatario:	Delegazioni
n. doc. prec.:	14954/22 + ADD 1
n. doc. Comm.:	8115/21
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione - Orientamento generale (6 dicembre 2022)

Si allega per le delegazioni l'orientamento generale del Consiglio sulla proposta in oggetto approvato dal Consiglio "Trasporti, telecomunicazioni e energia" nella 3917ª sessione tenutasi il 6 dicembre 2022.

L'orientamento generale definisce la posizione provvisoria del Consiglio su tale proposta e costituisce la base dei preparativi per i negoziati con il Parlamento europeo.

ALLEGATO

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 16 e 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[1],

visto il parere del Comitato delle regioni[2],

visto il parere della Banca centrale europea[3],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

[1] GU C […] del […], pag. […].
[2] GU C […] del […], pag. […].
[3] Riferimento al parere della BCE

(1) Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale (IA) in conformità dei valori dell'Unione. Il presente regolamento persegue una serie di motivi imperativi di interesse pubblico, quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento.

(2) I sistemi di intelligenza artificiale (sistemi di IA) possono essere facilmente impiegati in molteplici settori dell'economia e della società, anche a livello transfrontaliero, e circolare in tutta l'Unione. Alcuni Stati membri hanno già preso in esame l'adozione di regole nazionali per garantire che l'intelligenza artificiale sia sicura e sia sviluppata e utilizzata nel rispetto degli obblighi in materia di diritti fondamentali. Normative nazionali divergenti possono determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA. È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno, sulla base dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). Nella misura in cui il presente regolamento prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuno consultare il comitato europeo per la protezione dei dati.

(3) L'intelligenza artificiale consiste in una famiglia di tecnologie in rapida evoluzione che può contribuire al conseguimento di un'ampia gamma di benefici a livello economico e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale ed ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, istruzione e formazione, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, mitigazione dei cambiamenti climatici e adattamento ad essi.

(4) L'intelligenza artificiale può nel contempo, a seconda delle circostanze relative alla sua applicazione e al suo utilizzo specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti tutelati dalla legislazione dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale.

(5) Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di intelligenza artificiale per promuovere lo sviluppo, l'uso e l'adozione dell'intelligenza artificiale nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo, è opportuno stabilire regole che disciplinino l'immissione sul mercato e la messa in servizio di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi. Stabilendo tali regole e sulla base dei lavori del gruppo di esperti ad alto livello sull'intelligenza artificiale, come indicato negli Orientamenti per un'intelligenza artificiale affidabile nell'UE, il presente regolamento contribuisce all'obiettivo dell'Unione di essere un leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica, come affermato dal Consiglio europeo[4], e garantisce la tutela dei principi etici, come specificamente richiesto dal Parlamento europeo[5].

---

4 Consiglio europeo, riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni, EUCO 13/20, 2020, pag. 6.

5 Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

(5 bis) Le regole armonizzate concernenti l'immissione sul mercato, la messa in servizio e l'utilizzo dei sistemi di IA stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in linea con il suo approccio del nuovo quadro legislativo, non dovrebbero pregiudicare la normativa vigente dell'Unione, in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e sicurezza dei prodotti, a cui il presente regolamento è complementare. Di conseguenza, restano impregiudicati e pienamente applicabili tutti i diritti e i mezzi di ricorso concessi da tale normativa dell'Unione ai consumatori e ad altre persone che potrebbero subire l'impatto negativo dei sistemi di IA, anche per quanto riguarda il risarcimento di eventuali danni a norma della direttiva 85/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi. Inoltre, il presente regolamento mira a rafforzare l'efficacia di tali diritti e mezzi di ricorso esistenti definendo requisiti e obblighi specifici, anche per quanto riguarda la trasparenza, la documentazione tecnica e la conservazione delle registrazioni dei sistemi di IA. Oltre a ciò, gli obblighi imposti a vari operatori coinvolti nella catena del valore dell'IA a norma del presente regolamento dovrebbero applicarsi senza pregiudizio delle normative nazionali, in conformità del diritto dell'Unione, e avere l'effetto di limitare l'uso di determinati sistemi di IA qualora tali normative non rientrino nell'ambito di applicazione del presente regolamento o perseguano obiettivi legittimi di interesse pubblico diversi da quelli perseguiti dal presente regolamento. Ad esempio, il presente regolamento non dovrebbe incidere sulla normativa nazionale in materia di lavoro e sulle leggi in materia di protezione dei minori (ossia le persone di età inferiore ai 18 anni), tenendo conto del commento generale n. 25 delle Nazioni Unite (2021) sui diritti dei minori, nella misura in cui esse non riguardino in modo specifico i sistemi di IA e perseguano altri obiettivi legittimi di interesse pubblico.

(6) La nozione di sistema di IA dovrebbe essere definita in maniera chiara al fine di garantire la certezza del diritto, prevedendo nel contempo la flessibilità necessaria per agevolare i futuri sviluppi tecnologici. La definizione dovrebbe essere basata sulle principali caratteristiche funzionali dell'intelligenza artificiale, quali le sue capacità di apprendimento, ragionamento o modellizzazione, e distinguerla da sistemi software e approcci di programmazione più semplici. In particolare, ai fini del presente regolamento, i sistemi di IA dovrebbero avere la capacità, sulla base di input e dati elaborati dalle macchine e/o dall'uomo, di dedurre come raggiungere una serie di obiettivi finali che sono assegnati a tali sistemi dall'uomo, avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e di produrre output quali contenuti per sistemi di IA generativi (ad esempio testo, video o immagini), previsioni, raccomandazioni o decisioni, che influenzano l'ambiente con cui il sistema interagisce, tanto in una dimensione fisica quanto in una dimensione digitale. Un sistema che utilizza regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico non dovrebbe essere considerato un sistema di IA. I sistemi di IA possono essere progettati per funzionare con livelli di autonomia variabili e per essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato). Il concetto di autonomia di un sistema di IA si riferisce al grado di funzionamento di tale sistema senza il coinvolgimento umano.

(6 bis) Gli approcci di apprendimento automatico si concentrano sullo sviluppo di sistemi in grado di apprendere e dedurre dai dati per risolvere un problema di applicazione senza essere esplicitamente programmati con una serie di istruzioni passo-passo dall'input all'output. L'apprendimento si riferisce al processo computazionale di ottimizzazione dei parametri del modello a partire dai dati, una costruzione matematica che genera un output basato su dati di input. La gamma di problemi affrontati dall'apprendimento automatico comporta in genere compiti per i quali altri approcci falliscono, perché non vi è un'adeguata formalizzazione del problema o perché la risoluzione del problema è inscindibile da approcci non basati sull'apprendimento. Gli approcci basati sull'apprendimento automatico comprendono, ad esempio, l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, che utilizza una varietà di metodi, tra cui l'apprendimento profondo con reti neurali, le tecniche statistiche per l'apprendimento e l'inferenza (compresa, ad esempio, la regressione logistica, la stima bayesiana) e i metodi di ricerca e ottimizzazione.

(6 ter) Gli approcci basati sulla logica e sulla conoscenza si concentrano sullo sviluppo di sistemi con capacità di ragionamento logico sulla conoscenza per risolvere un problema di applicazione. Tali sistemi comportano generalmente una base di conoscenze e un motore inferenziale che genera output ragionando sulla base di conoscenze. La base di conoscenze, solitamente codificata da esperti umani, rappresenta entità e relazioni logiche pertinenti per il problema di applicazione attraverso formalismi basati su regole, ontologie o grafici di conoscenze. Il motore inferenziale agisce sulla base di conoscenze ed estrae nuove informazioni attraverso operazioni quali la cernita, la ricerca, l'abbinamento o il concatenamento. Gli approcci basati sulla logica e gli approcci basati sulla conoscenza comprendono ad esempio la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico), i sistemi esperti e i metodi di ricerca e ottimizzazione.

(6 quater) Al fine di garantire condizioni uniformi per l'attuazione del presente regolamento riguardo agli approcci di apprendimento automatico e agli approcci basati sulla logica e sulla conoscenza e per tenere conto degli sviluppi tecnologici e del mercato, è opportuno attribuire alla Commissione competenze di esecuzione.

(6 quinquies)La nozione di "utente" di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA e sotto la cui autorità è utilizzato il sistema. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dall'utente.

(7) La nozione di dati biometrici utilizzata nel presente regolamento dovrebbe essere interpretata in modo coerente con la nozione di dati biometrici di cui all'articolo 4, punto 14), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[6], all'articolo 3, punto 18), del regolamento (UE) n. 2018/1725 del Parlamento europeo e del Consiglio[7] e all'articolo 3, punto 13), della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[8].

[6] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[7] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

[8] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) (GU L 119 del 4.5.2016, pag. 89).

(8) È opportuno definire a livello funzionale la nozione di sistema di identificazione biometrica remota utilizzata nel presente regolamento, quale sistema di IA destinato all'identificazione tipicamente a distanza di persone fisiche, senza il loro coinvolgimento attivo, mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in un archivio di dati di riferimento, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati. Tali sistemi di identificazione biometrica remota sono generalmente utilizzati per percepire (scansionare) più persone o il loro comportamento simultaneamente al fine di facilitare in modo significativo l'identificazione di una serie di persone senza il loro coinvolgimento attivo. Tale definizione esclude i sistemi di verifica/autenticazione il cui unico scopo sarebbe quello di confermare che una determinata persona fisica è la persona che dichiara di essere, nonché i sistemi utilizzati per confermare l'identità di una persona fisica al solo scopo di avere accesso a un servizio, a un dispositivo o a un locale. Tale esclusione è giustificata dal fatto che detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone. Nel caso dei sistemi "in tempo reale", il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono tutti istantaneamente, quasi istantaneamente o in ogni caso senza ritardi significativi. A tale riguardo, non dovrebbe essere possibile eludere le regole del presente regolamento per quanto attiene all'uso "in tempo reale" dei sistemi di IA in questione prevedendo ritardi minimi. I sistemi "in tempo reale" comportano l'uso di materiale "dal vivo" o "quasi dal vivo" (ad esempio filmati) generato da una telecamera o da un altro dispositivo con funzionalità analoghe. Nel caso dei sistemi di identificazione "a posteriori", invece, i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono solo con un ritardo significativo. Si tratta di materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, che è stato generato prima che il sistema fosse usato in relazione alle persone fisiche interessate.

(9) Ai fini del presente regolamento, la nozione di spazio accessibile al pubblico dovrebbe essere intesa come riferita a qualsiasi luogo fisico accessibile a un numero indeterminato di persone fisiche, a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata e indipendentemente dall'attività per la quale il luogo può essere utilizzato, quali il commercio (ad esempio negozi, ristoranti, bar), i servizi (ad esempio banche, attività professionali, ospitalità), lo sport (ad esempio piscine, palestre, stadi), i trasporti (ad esempio stazioni di autobus, metropolitane e ferroviarie, aeroporti, mezzi di trasporto), l'intrattenimento (ad esempio cinema, teatri, musei, sale da concerto e sale conferenze), il tempo libero o altro (ad esempio strade e piazze pubbliche, parchi, foreste, parchi giochi). Un luogo dovrebbe essere classificato come accessibile al pubblico anche se, indipendentemente da potenziali restrizioni di capacità o di sicurezza, l'accesso è soggetto a talune condizioni predeterminate, che possono essere soddisfatte da un numero indeterminato di persone, quali l'acquisto di un biglietto o titolo di trasporto, la registrazione precedente o il raggiungimento di una determinata età. Per contro, un luogo non dovrebbe essere considerato accessibile al pubblico se l'accesso è limitato a persone fisiche specifiche e definite attraverso la normativa dell'Unione o nazionale direttamente connessa alla pubblica sicurezza o attraverso la chiara manifestazione di volontà da parte della persona che ha l'autorità pertinente sul luogo. La sola possibilità concreta di accesso (ad esempio una porta sbloccata, un cancello aperto in una recinzione) non implica che il luogo sia accessibile al pubblico in presenza di indicazioni o circostanze che suggeriscono il contrario (ad esempio segnaletica che vieta o limita l'accesso). I locali delle imprese e delle fabbriche, come pure gli uffici e i luoghi di lavoro destinati ad essere accessibili solo dai pertinenti dipendenti e prestatori di servizi, sono luoghi non accessibili al pubblico. Gli spazi accessibili al pubblico non dovrebbero includere le carceri o le zone adibite ai controlli di frontiera. Alcune altre zone possono essere composte sia da aree non accessibili al pubblico che da aree accessibili al pubblico, come l'atrio di un edificio residenziale privato da cui è possibile accedere a uno studio medico o a un aeroporto. Non sono del pari contemplati gli spazi online, dato che non sono luoghi fisici. L'accessibilità di un determinato spazio al pubblico dovrebbe tuttavia essere determinata caso per caso, tenendo conto delle specificità della singola situazione presa in esame.

(10) Al fine di garantire condizioni di parità e una protezione efficace dei diritti e delle libertà delle persone in tutta l'Unione, è opportuno che le regole stabilite dal presente regolamento si applichino ai fornitori di sistemi di IA in modo non discriminatorio, a prescindere dal fatto che siano stabiliti nell'Unione o in un paese terzo, e agli utenti dei sistemi di IA stabiliti nell'Unione.

(11) Alla luce della loro natura di sistemi digitali, è opportuno che determinati sistemi di IA rientrino nell'ambito di applicazione del presente regolamento anche quando non sono immessi sul mercato, né messi in servizio, né utilizzati nell'Unione. È il caso, ad esempio, di un operatore stabilito nell'Unione che appalta alcuni servizi a un operatore stabilito al di fuori dell'Unione in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio. In tali circostanze il sistema di IA utilizzato dall'operatore al di fuori dell'Unione potrebbe trattare dati raccolti nell'Unione e da lì trasferiti, nel rispetto della legge, e fornire all'operatore appaltante nell'Unione l'output di tale sistema di IA risultante da tale trattamento, senza che tale sistema di IA sia immesso sul mercato, messo in servizio o utilizzato nell'Unione. Al fine di impedire l'elusione del presente regolamento e di garantire una protezione efficace delle persone fisiche che si trovano nell'Unione, è opportuno che il presente regolamento si applichi anche ai fornitori e agli utenti di sistemi di IA stabiliti in un paese terzo, nella misura in cui l'output prodotto da tali sistemi è utilizzato nell'Unione. Cionondimeno, per tener conto degli accordi vigenti e delle esigenze particolari per la cooperazione futura con partner stranieri con cui sono scambiate informazioni e elementi probatori, il presente regolamento non dovrebbe applicarsi alle autorità pubbliche di un paese terzo e alle organizzazioni internazionali che agiscono nel quadro di accordi internazionali conclusi a livello nazionale o europeo per la cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con i suoi Stati membri. Tali accordi sono stati conclusi bilateralmente tra Stati membri e paesi terzi o tra l'Unione europea, Europol e altre agenzie dell'UE e paesi terzi e organizzazioni internazionali. Le autorità degli Stati membri destinatari e le istituzioni, gli organi e gli organismi dell'Unione nonché gli organismi che si avvalgono di tali output nell'Unione, restano responsabili di garantire che il loro utilizzo sia conforme alla normativa dell'Unione. In caso di revisione di tali accordi internazionali o di conclusione di nuovi accordi internazionali in futuro, le parti contraenti dovrebbero adoperarsi quanto più possibile per allineare tali accordi ai requisiti del presente regolamento.

(12) È altresì opportuno che il presente regolamento si applichi alle istituzioni, agli organi e agli organismi dell'Unione quando agiscono in qualità di fornitori o utenti di un sistema di IA.

(-12 bis) Se, e nella misura in cui, i sistemi di IA sono immessi sul mercato, messi in servizio o utilizzati con o senza modifica di tali sistemi per scopi militari, di difesa o di sicurezza nazionale, essi dovrebbero essere esclusi dall'ambito di applicazione del presente regolamento indipendentemente dal tipo di entità che svolge tali attività, ad esempio se si tratta di un'entità pubblica o privata. Per quanto riguarda gli scopi militari e di difesa, tale esclusione è giustificata sia dall'articolo 4, paragrafo 2, TUE sia dalle specificità della politica di difesa comune degli Stati membri e dell'Unione di cui al titolo V, capo 2, del trattato sull'Unione europea (TUE) che sono soggette al diritto internazionale pubblico, che costituisce pertanto il quadro giuridico più appropriato per la regolamentazione dei sistemi di IA nel contesto dell'uso letale della forza e di altri sistemi di IA nel contesto delle attività militari e di difesa. Per quanto riguarda le finalità di sicurezza nazionale, l'esclusione è giustificata sia dal fatto che la sicurezza nazionale resta di esclusiva competenza degli Stati membri ai sensi dell'articolo 4, paragrafo 2, TUE, sia dalla natura specifica e dalle esigenze operative delle attività di sicurezza nazionale, nonché dalle specifiche norme nazionali applicabili a tali attività. Tuttavia, se un sistema di IA sviluppato, immesso sul mercato, messo in servizio o utilizzato per scopi militari, di difesa o di sicurezza nazionale è usato al di fuori di tali finalità, in via temporanea o permanente per altri scopi (ad esempio a fini civili o umanitari, per scopi di attività di contrasto o di sicurezza pubblica), tale sistema rientrerebbe nell'ambito di applicazione del presente regolamento. In tal caso, l'entità che utilizza il sistema per finalità diverse da quelle militari, di difesa o di sicurezza nazionale dovrebbe garantire la conformità del sistema al presente regolamento, a meno che il sistema non sia già conforme al presente regolamento. Rientrano nell'ambito di applicazione del presente regolamento i sistemi di IA immessi sul mercato o messi in servizio per una finalità esclusa (ossia militare, di difesa o di sicurezza nazionale) e per una o più finalità non escluse (ad esempio scopi civili, attività di contrasto ecc.) e i fornitori di tali sistemi dovrebbero garantire la conformità al presente regolamento. In tali casi, il fatto che un sistema di IA possa rientrare nell'ambito di applicazione del presente regolamento non dovrebbe incidere sulla possibilità per le entità che svolgono attività militari, di sicurezza nazionale e di difesa, indipendentemente dal tipo di entità che svolge tali attività, di utilizzare sistemi di IA per scopi di sicurezza nazionale, militari e di difesa, l'uso dei quali è escluso dall'ambito di applicazione del presente regolamento. Un sistema di IA immesso sul mercato per scopi civili o di attività di contrasto che è utilizzato con o senza modifiche a fini militari, di difesa o di sicurezza nazionale non dovrebbe rientrare nell'ambito di applicazione del presente regolamento, indipendentemente dal tipo di entità che svolge tali attività.

(12 bis) Il presente regolamento non dovrebbe pregiudicare le disposizioni relative alla responsabilità dei prestatori intermediari di cui alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio [come modificata dalla legge sui servizi digitali].

(12 ter) Il presente regolamento non dovrebbe pregiudicare le attività di ricerca e sviluppo e dovrebbe rispettare la libertà della scienza. È pertanto necessario escludere dal suo ambito di applicazione i sistemi di IA specificamente sviluppati e messi in servizio solo a scopo di ricerca e sviluppo in ambito scientifico e garantire che il regolamento non incida altrimenti sulle attività scientifiche di ricerca e sviluppo relative ai sistemi di IA. Le disposizioni del presente regolamento non dovrebbero applicarsi anche per quanto concerne l'attività di ricerca orientata ai prodotti svolta dai fornitori. Ciò non pregiudica l'obbligo di conformarsi al presente regolamento quando un sistema di IA che rientra nell'ambito di applicazione del presente regolamento è immesso sul mercato o messo in servizio in conseguenza di tale attività di ricerca e sviluppo, così come non pregiudica l'applicazione delle disposizioni sugli spazi di sperimentazione normativa e sulle prove in condizioni reali. Inoltre, fatto salvo quanto precede riguardo ai sistemi di IA specificamente sviluppati e messi in servizio solo a scopo di ricerca e sviluppo in ambito scientifico, qualsiasi altro sistema di IA che possa essere utilizzato per lo svolgimento di qualsiasi attività di ricerca e sviluppo dovrebbe rimanere soggetto alle disposizioni del presente regolamento. In ogni circostanza, qualsiasi attività di ricerca e sviluppo dovrebbe essere svolta conformemente alle norme etiche e professionali riconosciute nell'ambito della ricerca scientifica.

(12 quater) Alla luce della natura e della complessità della catena del valore dei sistemi di IA, è essenziale chiarire il ruolo degli attori che possono contribuire allo sviluppo dei sistemi di IA, specie dei sistemi di IA ad alto rischio. In particolare, è necessario chiarire che i sistemi di IA per finalità generali sono sistemi di IA destinati secondo le intenzioni del fornitore a svolgere funzioni di applicazione generale, quali il riconoscimento di immagini o vocale, in una pluralità di contesti. Possono essere utilizzati da soli come sistemi di IA ad alto rischio o essere componenti di altri sistemi di IA ad alto rischio. Pertanto, data la loro natura particolare e al fine di garantire un'equa ripartizione delle responsabilità lungo la catena del valore dell'IA, tali sistemi dovrebbero essere soggetti a requisiti e obblighi proporzionati e più specifici a norma del presente regolamento, garantendo nel contempo un elevato livello di protezione dei diritti fondamentali, della salute e della sicurezza. Inoltre, i fornitori di sistemi di IA per finalità generali, indipendentemente dal fatto che questi possano essere utilizzati di per sé come sistemi di IA ad alto rischio da altri fornitori o come componenti di sistemi di IA ad alto rischio, dovrebbero cooperare, a seconda dei casi, con i fornitori dei rispettivi sistemi di IA ad alto rischio per consentire loro di rispettare i pertinenti obblighi previsti dal presente regolamento e con le autorità competenti istituite a norma del presente regolamento. Al fine di tenere conto delle caratteristiche specifiche dei sistemi di IA per finalità generali e degli sviluppi tecnologici e di mercato in rapida evoluzione nel settore, è opportuno attribuire alla Commissione competenze di esecuzione per specificare e adattare l'applicazione dei requisiti stabiliti a norma del presente regolamento ai sistemi di IA per finalità generali e per specificare le informazioni che i fornitori di sistemi di IA per finalità generali sono tenuti a condividere in modo da consentire ai fornitori del rispettivo sistema di IA ad alto rischio di rispettare i loro obblighi a norma del presente regolamento.

(13) Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire norme legislative comuni per tutti i sistemi di IA ad alto rischio. Tali norme dovrebbero essere coerenti con la Carta dei diritti fondamentali dell'Unione europea (la Carta), non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione.

(14) Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di intelligenza artificiale, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA.

(15) L'intelligenza artificiale presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e dovrebbero essere vietate poiché contraddicono i valori dell'Unione relativi al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia e dello Stato di diritto e dei diritti fondamentali dell'Unione, compresi il diritto alla non discriminazione, alla protezione dei dati e della vita privata e i diritti dei minori.

(16) Le tecniche di manipolazione basate sull'IA possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la scelta. È opportuno vietare, in quanto particolarmente pericolosi, l'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA che distorcono materialmente il comportamento umano e che possono provocare danni fisici o psicologici. Tali sistemi di IA impiegano componenti subliminali quali stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli vanno al di là della percezione umana o altre tecniche subliminali che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona senza che ne sia consapevole o, anche se ne è consapevole, senza che sia in grado di controllarle o resistervi, ad esempio in caso di interfacce cervello-computer o di realtà virtuale. In aggiunta, i sistemi di IA possono inoltre sfruttare in altro modo le vulnerabilità di uno specifico gruppo di persone dovute all'età, a disabilità ai sensi della direttiva (UE) 2019/882 o a una specifica situazione sociale o economica che potrebbe rendere tali persone più vulnerabili allo sfruttamento, come le persone che vivono in condizioni di povertà estrema e le minoranze etniche o religiose. Tali sistemi di IA possono essere immessi sul mercato, messi in servizio o utilizzati con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona e in un modo che provochi o possa verosimilmente provocare a tale persona o a un'altra persona o gruppo di persone un danno fisico o psicologico, compresi i danni che possono essere accumulati nel tempo. Tale intento di distorcere il comportamento non può essere presunto se la distorsione è determinata da fattori esterni al sistema di IA, che sfuggono al controllo del fornitore o dell'utente, ossia fattori che possono non essere ragionevolmente previsti e attenuati dal fornitore o dall'utente del sistema di IA. In ogni caso, non è necessario che il fornitore o l'utente abbiano l'intento di provocare il danno fisico o psicologico, purché tale danno derivi da pratiche manipolative o di sfruttamento consentite dall'IA. Il divieto di tali pratiche di IA è complementare alle disposizioni contenute nella direttiva 2005/29/CE, in particolare le pratiche commerciali sleali che comportano danni economici o finanziari per i consumatori sono vietate in ogni circostanza, indipendentemente dal fatto che siano attuate attraverso sistemi di IA o in altro modo. I divieti di pratiche manipolative e di sfruttamento di cui al presente regolamento non dovrebbero pregiudicare le pratiche lecite nel contesto di trattamenti medici, quali il trattamento psicologico di una malattia mentale o la riabilitazione fisica, quando tali pratiche sono svolte conformemente alle norme e leggi applicabili in ambito medico. Inoltre, le pratiche commerciali comuni e legittime che sono conformi alla normativa applicabile non dovrebbero essere considerate di per sé come pratiche di IA manipolative o dannose.

(17) I sistemi di IA che permettono alle autorità pubbliche o ad attori privati di attribuire un punteggio sociale alle persone fisiche possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano le persone fisiche sulla base del loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note o previste. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio dovrebbero pertanto essere vietati. Tale divieto non dovrebbe pregiudicare le pratiche lecite di valutazione delle persone fisiche effettuate per uno o più scopi specifici nel rispetto della legge.

(18) L'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto è ritenuto particolarmente invasivo dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali. L'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi che operano "in tempo reale" comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone oggetto di attività di contrasto.

(19) L'uso di tali sistemi a fini di attività di contrasto dovrebbe pertanto essere vietato, eccezion fatta per le situazioni elencate in modo esaustivo e definite rigorosamente, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi. Tali situazioni comprendono la ricerca di potenziali vittime di reato, compresi i minori scomparsi, determinate minacce per la vita o l'incolumità fisica delle persone fisiche o un attacco terroristico nonché il rilevamento, la localizzazione e l'identificazione degli autori o dei sospettati di reati di cui nella decisione quadro 2002/584/GAI del Consiglio[9] o l'azione penale nei loro confronti, se tali reati, quali definiti dalla legge dello Stato membro interessato, sono punibili in tale Stato membro con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno tre anni. Tale soglia per la pena o la misura di sicurezza privativa della libertà personale in conformità al diritto nazionale contribuisce a garantire che il reato sia sufficientemente grave da giustificare potenzialmente l'uso di sistemi di identificazione biometrica remota "in tempo reale". Inoltre è probabile che, a livello pratico, alcuni dei 32 reati elencati della decisione quadro 2002/584/GAI del Consiglio risultino più pertinenti di altri, poiché il grado di necessità e proporzionalità del ricorso all'identificazione biometrica remota "in tempo reale" sarà prevedibilmente molto variabile per quanto concerne il perseguimento pratico del rilevamento, della localizzazione, dell'identificazione o dell'azione penale nei confronti di un autore o un sospettato dei vari reati elencati e con riguardo alle possibili differenze in termini di gravità, probabilità e portata del danno o delle eventuali conseguenze negative. Il presente regolamento dovrebbe altresì preservare la capacità delle autorità di contrasto e delle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo di svolgere controlli d'identità in presenza della persona interessata, conformemente alle condizioni stabilite per tali controlli dal diritto dell'Unione e nazionale. In particolare, le autorità di contrasto e le autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo dovrebbero poter utilizzare i sistemi di informazione, conformemente al diritto dell'Unione o nazionale, per identificare una persona che, durante un controllo d'identità, rifiuta di essere identificata o non è in grado di dichiarare o dimostrare la propria identità, senza essere tenute, a norma del presente regolamento, a ottenere un'autorizzazione preventiva. Potrebbe trattarsi, ad esempio, di una persona coinvolta in un reato che, a causa di un incidente o di un problema di salute, non vuole rivelare la propria identità alle autorità di contrasto o non è in grado di farlo.

---

[9] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

(20) Al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, è altresì importante stabilire che, in ciascuna delle situazioni elencate in modo esaustivo e definite rigorosamente, è opportuno tener conto di taluni elementi, in particolare per quanto riguarda la natura della situazione all'origine della richiesta e le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate, nonché le tutele e le condizioni previste per l'uso. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto dovrebbe inoltre essere subordinato a limiti di tempo e di spazio adeguati, con particolare riguardo a indicazioni o elementi probatori relativi a minacce, vittime o autori di reati. La banca dati di riferimento delle persone dovrebbe risultare adeguata per ogni caso d'uso in ciascuna delle situazioni di cui sopra.

(21) È opportuno subordinare ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a un'autorizzazione esplicita e specifica da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente di uno Stato membro. Tale autorizzazione dovrebbe, in linea di principio, essere ottenuta prima dell'uso del sistema al fine di identificare una o più persone. Eccezioni a tale regola dovrebbero essere ammesse in situazioni di urgenza debitamente giustificate, vale a dire le situazioni in cui la necessità di utilizzare i sistemi in questione è tale da far sì che sia effettivamente e oggettivamente impossibile ottenere un'autorizzazione prima di iniziare a utilizzare il sistema. In tali situazioni di urgenza, è opportuno limitare l'uso al minimo indispensabile e subordinarlo a tutele e condizioni adeguate, come stabilito dal diritto nazionale e specificato nel contesto di ogni singolo caso d'uso urgente dall'autorità di contrasto stessa. L'autorità di contrasto dovrebbe inoltre in tali situazioni tentare di ottenere nel minor tempo possibile un'autorizzazione, indicando contestualmente i motivi per cui non ha potuto richiederla prima.

(22) È altresì opportuno prevedere, nell'ambito del quadro esaustivo stabilito dal presente regolamento, che tale uso nel territorio di uno Stato membro in conformità al presente regolamento sia possibile solo nel caso e nella misura in cui lo Stato membro in questione abbia deciso di prevedere espressamente la possibilità di autorizzare tale uso nelle regole dettagliate del proprio diritto nazionale. Gli Stati membri restano di conseguenza liberi, a norma del presente regolamento, di non prevedere affatto tale possibilità o di prevederla soltanto per alcuni degli obiettivi idonei a giustificare l'uso autorizzato di cui nel presente regolamento.

(23) L'uso di sistemi di IA per l'identificazione biometrica remota "in tempo reale" di persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto comporta necessariamente il trattamento di dati biometrici. Le regole del presente regolamento che, fatte salve alcune eccezioni, vietano tale uso, e che sono basate sull'articolo 16 TFUE, dovrebbero applicarsi come *lex specialis* rispetto alle regole sul trattamento dei dati biometrici di cui all'articolo 10 della direttiva (UE) 2016/680, disciplinando quindi in modo esaustivo tale uso e il trattamento dei dati biometrici interessati. L'uso e il trattamento di cui sopra dovrebbero pertanto essere possibili solo nella misura in cui siano compatibili con il quadro stabilito dal presente regolamento, senza che al di fuori di tale quadro sia prevista la possibilità, per le autorità competenti, quando agiscono a fini di attività di contrasto, di utilizzare tali sistemi e trattare tali dati in connessione con tali attività per i motivi di cui all'articolo 10 della direttiva (UE) 2016/680. In tale contesto, il presente regolamento non è inteso a fornire la base giuridica per il trattamento dei dati personali a norma dell'articolo 8 della direttiva 2016/680. Tuttavia, l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini diversi dalle attività di contrasto, anche da parte delle autorità competenti, non dovrebbe rientrare nel quadro specifico stabilito dal presente regolamento in relazione a tale uso a fini di attività di contrasto. Tale uso a fini diversi dalle attività di contrasto non dovrebbe pertanto essere subordinato all'obbligo di un'autorizzazione a norma del presente regolamento e delle regole dettagliate applicabili del diritto nazionale che possono darvi attuazione.

(24) Qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal presente regolamento, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 10 della direttiva (UE) 2016/680. Per finalità diverse dalle attività di contrasto, l'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e l'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 vietano il trattamento di dati biometrici intesi a identificare in modo univoco una persona fisica, a meno che non si applichi una delle situazioni di cui al rispettivo secondo paragrafo di tali articoli.

(25) A norma dell'articolo 6 bis del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, l'Irlanda non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, lettera d), e paragrafi 2, 3 e 4, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, laddove l'Irlanda non sia vincolata da regole che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 TFUE.

(26) A norma degli articoli 2 e 2 bis del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, la Danimarca non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, lettera d), e paragrafi 2, 3 e 4, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, né è soggetta alla loro applicazione.

(27) È opportuno che i sistemi di IA ad alto rischio siano immessi sul mercato dell'Unione o messi in servizio solo se soddisfano determinati requisiti obbligatori. Tali requisiti dovrebbero garantire che i sistemi di IA ad alto rischio disponibili nell'Unione o i cui output sono altrimenti utilizzati nell'Unione non presentino rischi inaccettabili per interessi pubblici importanti dell'Unione, come riconosciuti e tutelati dal diritto dell'Unione. È opportuno limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione, e tale limitazione riduce al minimo eventuali potenziali restrizioni al commercio internazionale.

(28) I sistemi di IA potrebbero avere ripercussioni negative per la salute e la sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati. La portata dell'impatto negativo del sistema di IA sui diritti fondamentali protetti dalla Carta è di particolare rilevanza ai fini della classificazione di un sistema di IA tra quelli ad alto rischio. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e la non discriminazione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione. Oltre a tali diritti, è importante sottolineare che i minori godono di diritti specifici sanciti dall'articolo 24 della Carta dell'UE e dalla Convenzione delle Nazioni Unite sui diritti del fanciullo (ulteriormente elaborati nell'osservazione generale n. 25 della Convenzione delle Nazioni Unite sui diritti del fanciullo per quanto riguarda l'ambiente digitale), che prevedono la necessità di tenere conto delle loro vulnerabilità e di fornire la protezione e l'assistenza necessarie al loro benessere. È altresì opportuno tenere in considerazione, nel valutare la gravità del danno che un sistema di IA può provocare, anche in relazione alla salute e alla sicurezza delle persone, il diritto fondamentale a un livello elevato di protezione dell'ambiente sancito dalla Carta e attuato nelle politiche dell'Unione.

(29) Per quanto riguarda i sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti o sistemi o che sono essi stessi prodotti o sistemi che rientrano nell'ambito di applicazione del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio[10], del regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio[11], del regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio[12], della direttiva 2014/90/UE del Parlamento europeo e del Consiglio[13], della direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio[14], del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio[15], del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio[16], e del regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio[17], è opportuno modificare i suddetti atti per garantire che, nell'adottare qualsiasi futuro atto delegato o di esecuzione pertinente sulla base di tali atti, la Commissione tenga conto, sulla base delle specificità tecniche e normative di ciascun settore e senza interferire con i vigenti meccanismi di governance, valutazione della conformità e applicazione e con le autorità da essi stabilite, dei requisiti obbligatori sanciti dal presente regolamento.

---

10 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).

11 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).

12 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).

13 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).

14 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).

15 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).

16 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).

17 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).

(30) Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto in questione è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici e dispositivi medico-diagnostici in vitro.

(31) La classificazione di un sistema di IA come ad alto rischio a norma del presente regolamento non dovrebbe necessariamente significare che il prodotto il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia considerato "ad alto rischio" in base ai criteri stabiliti nella pertinente normativa di armonizzazione dell'Unione che si applica al prodotto. Ciò vale in particolare per il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio[18] e per il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio[19], in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio.

---

18 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).

19 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).

(32) Per quanto riguarda i sistemi di IA ad alto rischio diversi da quelli che sono componenti di sicurezza di prodotti o che sono essi stessi prodotti, è opportuno classificarli come ad alto rischio se, alla luce della loro finalità prevista, presentano un alto rischio di pregiudicare la salute e la sicurezza o i diritti fondamentali delle persone, tenendo conto sia della gravità del possibile danno sia della probabilità che si verifichi, e sono utilizzati in una serie di settori specificamente predefiniti indicati nel regolamento. L'identificazione di tali sistemi si basa sulla stessa metodologia e sui medesimi criteri previsti anche per eventuali future modifiche dell'elenco dei sistemi di IA ad alto rischio. È altresì importante chiarire che negli scenari ad alto rischio di cui all'allegato III possono esservi sistemi che non comportano un rischio significativo per gli interessi giuridici tutelati nell'ambito di tali scenari, tenendo conto dell'output prodotto dal sistema di IA. Pertanto, il sistema di IA che genera tale output dovrebbe essere considerato ad alto rischio solo quando tale output ha un elevato grado di importanza (ossia non è puramente accessorio) in relazione all'azione o alla decisione pertinente, tale da generare un rischio significativo per gli interessi giuridici tutelati. Ad esempio, quando le informazioni fornite da un sistema di IA all'uomo consistono nella profilazione delle persone fisiche ai sensi dell'articolo 4, punto 4, del regolamento (UE) 2016/679, dell'articolo 3, punto 4, della direttiva (UE) 2016/680 e dell'articolo 3, punto 5, del regolamento (UE) 2018/1725, tali informazioni non dovrebbero di norma essere considerate di natura accessoria nel contesto dei sistemi di IA ad alto rischio di cui all'allegato III. Tuttavia, se l'output del sistema di IA ha solo una rilevanza minore o trascurabile per l'azione o la decisione umana, esso può essere considerato puramente accessorio, compresi, ad esempio, i sistemi di IA utilizzati per la traduzione a fini informativi o per la gestione di documenti.

(33) Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Ciò diviene particolarmente importante quando si trattano aspetti quali età, etnia, razza, sesso o disabilità. È pertanto opportuno classificare i sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori" come sistemi ad alto rischio. Alla luce dei rischi che comportano, entrambi i tipi di sistemi di identificazione biometrica remota dovrebbero essere soggetti a requisiti specifici in materia di capacità di registrazione e sorveglianza umana.

(34) Per quanto riguarda la gestione e il funzionamento delle infrastrutture critiche, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati come componenti di sicurezza ai fini della gestione e del funzionamento delle infrastrutture digitali critiche di cui all'allegato I, punto 8, della direttiva sulla resilienza dei soggetti critici, del traffico stradale nonché della fornitura di acqua, gas, riscaldamento ed elettricità, in quanto un loro guasto o malfunzionamento può mettere a rischio la vita e la salute di un grande numero di persone e provocare perturbazioni significative del normale svolgimento delle attività sociali ed economiche. I componenti di sicurezza delle infrastrutture critiche, comprese le infrastrutture digitali critiche, sono sistemi utilizzati per proteggere direttamente l'integrità fisica delle infrastrutture critiche ovvero la salute e la sicurezza delle persone e dei beni ma che non sono necessari per il funzionamento del sistema. Un guasto o malfunzionamento di tali componenti potrebbe comportare direttamente rischi per l'integrità fisica delle infrastrutture critiche e quindi per la salute e la sicurezza delle persone e dei beni. I componenti destinati a essere utilizzati esclusivamente a fini di cibersicurezza non dovrebbero essere considerati componenti di sicurezza. Tra gli esempi di componenti di sicurezza di tali infrastrutture critiche possono rientrare i sistemi di monitoraggio della pressione idrica o sistemi di controllo degli incendi nei centri di cloud computing.

(35) I sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso, l'ammissione o l'assegnazione di persone agli istituti o programmi di istruzione e formazione professionale a tutti i livelli o per valutare i risultati dell'apprendimento delle persone, dovrebbero essere considerati ad alto rischio in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione.

(36) Anche i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per l'assunzione e la selezione delle persone, per l'adozione di decisioni in materia di promozione e cessazione del rapporto di lavoro, nonché per l'assegnazione dei compiti, sulla base del comportamento individuale o dei tratti e delle caratteristiche personali, per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro, dovrebbero essere classificati come sistemi ad alto rischio, in quanto tali sistemi possono avere un impatto significativo sul futuro di tali persone in termini di future prospettive di carriera e sostentamento. I pertinenti rapporti contrattuali legati al lavoro dovrebbero coinvolgere i dipendenti e le persone che forniscono servizi tramite piattaforme, come indicato nel programma di lavoro annuale della Commissione per il 2021. In linea di principio, tali persone non dovrebbero essere considerate utenti ai sensi del presente regolamento. Durante tutto il processo di assunzione, nonché ai fini della valutazione e della promozione delle persone o del proseguimento dei rapporti contrattuali legati al lavoro, tali sistemi possono perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale. I sistemi di IA utilizzati per monitorare le prestazioni e il comportamento di tali persone possono inoltre incidere sui loro diritti in materia di protezione dei dati e vita privata.

(37) Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni prestazioni e servizi pubblici e servizi privati essenziali, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. È in particolare opportuno classificare i sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche come sistemi di IA ad alto rischio, in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. I sistemi di IA utilizzati a tal fine possono portare alla discriminazione di persone o gruppi e perpetuare modelli storici di discriminazione, ad esempio in base all'origine razziale o etnica, alle disabilità, all'età o all'orientamento sessuale, o dar vita a nuove forme di effetti discriminatori. In considerazione della portata molto limitata dell'impatto e delle alternative disponibili sul mercato, è opportuno esentare i sistemi di IA destinati alla valutazione dell'affidabilità creditizia e del merito creditizio nei casi in cui sono messi in servizio da microimprese o piccole imprese, secondo la definizione di cui all'allegato della raccomandazione 2003/361/CE della Commissione, per uso proprio. Le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità competenti. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere negati, ridotti, revocati o recuperati dalle autorità, compreso se i beneficiari hanno legittimamente diritto a tali prestazioni o servizi, possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana o a un ricorso effettivo. È pertanto opportuno classificare tali sistemi come sistemi ad alto rischio. Cionondimeno, il presente regolamento non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche. Infine, è opportuno classificare come ad alto rischio anche i sistemi di IA utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, in quanto prendono decisioni in situazioni molto critiche per la vita e la salute delle persone e per i loro beni. I sistemi di IA sono inoltre sempre più utilizzati per la valutazione dei rischi in relazione alle persone fisiche e alla determinazione dei prezzi nel caso di assicurazioni sulla vita e assicurazioni sanitarie: se non debitamente progettati, sviluppati e utilizzati, possono comportare gravi conseguenze per la vita e la salute delle persone, tra cui la discriminazione e l'esclusione finanziaria. Al fine di garantire un approccio coerente nel settore dei servizi finanziari, dovrebbe applicarsi la suddetta eccezione per le microimprese o le piccole imprese per uso proprio, nella misura in cui esse stesse forniscono e mettono in servizio un sistema di IA allo scopo di vendere i propri prodotti assicurativi.

(38) Le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta. In particolare, il sistema di IA, se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di accuratezza o robustezza, o se non è adeguatamente progettato e sottoposto a prova prima di essere immesso sul mercato o altrimenti messo in servizio, può individuare le persone in modo discriminatorio o altrimenti errato o ingiusto. Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati. È pertanto opportuno classificare come ad alto rischio una serie di sistemi di IA destinati a essere utilizzati nel contesto delle attività di contrasto, in cui l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci. In considerazione della natura delle attività in questione e dei rischi a esse connessi, tra tali sistemi di IA ad alto rischio è opportuno includere, in particolare, i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto per valutazioni dei rischi individuali, come poligrafi e strumenti analoghi, oppure per rilevare lo stato emotivo delle persone fisiche, valutare l'affidabilità degli elementi probatori nei procedimenti penali, prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale sulla base della profilazione delle persone fisiche, o valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso delle persone fisiche o dei gruppi, nonché ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati. I sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali, come pure dalle unità di informazione finanziaria che svolgono compiti amministrativi di analisi delle informazioni conformemente alla normativa antiriciclaggio dell'Unione, non dovrebbero essere considerati sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati.

(39) I sistemi di IA utilizzati nella gestione della migrazione, dell'asilo e del controllo delle frontiere hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione. È pertanto opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti incaricate di compiti in materia di gestione della migrazione, dell'asilo e del controllo delle frontiere, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica, per valutare taluni rischi presentati da persone fisiche che entrano nel territorio di uno Stato membro o presentano domanda di visto o di asilo, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami per quanto riguarda l'obiettivo di determinare l'ammissibilità delle persone fisiche che richiedono tale status. I sistemi di IA nel settore della gestione della migrazione, dell'asilo e dei controlli di frontiera di cui al presente regolamento dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dalla direttiva 2013/32/UE del Parlamento europeo e del Consiglio[20], dal regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio[21] e da altre normative pertinenti.

---

20 Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU L 180 del 29.6.2013, pag. 60).

21 Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un Codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

(40) Alcuni sistemi di IA destinati all'amministrazione della giustizia e ai processi democratici dovrebbero essere classificati come sistemi ad alto rischio, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale. È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati ad assistere le autorità giudiziarie nelle attività di interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti. Non è tuttavia opportuno estendere tale classificazione ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi.

(41) Il fatto che un sistema di IA sia classificato come ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità ai requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale. Il presente regolamento non dovrebbe essere inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali, salvo quando diversamente disposto in modo specifico dal presente regolamento.

(42) Al fine di attenuare i rischi derivanti dai sistemi di IA ad alto rischio immessi o altrimenti messi in servizio sul mercato dell'Unione, è opportuno applicare determinati requisiti obbligatori, tenendo conto della finalità prevista dell'uso del sistema e conformemente al sistema di gestione dei rischi che deve essere stabilito dal fornitore. In particolare, il sistema di gestione dei rischi dovrebbe essere costituito da un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio. Tale processo dovrebbe garantire che il fornitore individui e analizzi i rischi per la salute, la sicurezza e i diritti fondamentali delle persone che possono essere interessate dal sistema alla luce della sua finalità prevista, compresi gli eventuali rischi derivanti dall'interazione tra il sistema di IA e l'ambiente in cui opera, e adotti di conseguenza adeguate misure di gestione dei rischi alla luce dello stato dell'arte.

(43) Tali requisiti dovrebbero applicarsi ai sistemi di IA ad alto rischio per quanto concerne la qualità dei set di dati utilizzati, la documentazione tecnica e la conservazione delle registrazioni, la trasparenza e la fornitura di informazioni agli utenti, la sorveglianza umana e la robustezza, l'accuratezza e la cibersicurezza. Tali requisiti sono necessari per attenuare efficacemente i rischi per la salute, la sicurezza e i diritti fondamentali, come applicabile alla luce della finalità prevista del sistema, e, non essendo ragionevolmente disponibili altre misure meno restrittive degli scambi, sono così evitate limitazioni ingiustificate del commercio.

(44) Un'elevata qualità dei dati è essenziale per le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi fonte di una discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessaria l'attuazione di adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento, convalida e prova dovrebbero essere sufficientemente pertinenti e rappresentativi e possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Tali set di dati dovrebbero inoltre essere quanto più possibile esenti da errori e completi in considerazione della finalità prevista del sistema di IA, tenendo conto in modo proporzionato della fattibilità tecnica e dello stato dell'arte, della disponibilità dei dati e dell'attuazione di adeguate misure di gestione dei rischi, in modo da affrontare debitamente le eventuali carenze del set di dati. Il requisito secondo cui i set di dati dovrebbero essere completi ed esenti da errori non dovrebbe incidere sull'uso di tecniche di tutela della vita privata nel contesto dello sviluppo e delle prove dei sistemi di IA. I set di dati di addestramento, convalida e prova dovrebbero tenere conto, nella misura richiesta dalla finalità prevista, delle caratteristiche o degli elementi peculiari dello specifico contesto o ambito geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato. Al fine di proteggere i diritti di terzi dalla discriminazione che potrebbe derivare dalla distorsione nei sistemi di IA, è opportuno che i fornitori siano in grado di trattare anche categorie particolari di dati personali, come questione di interesse pubblico rilevante ai sensi dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 e dell'articolo 10, paragrafo 2, lettera g), del regolamento (UE) 2018/1725, al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio.

(44 bis) Nell'applicare i principi di cui all'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679 e all'articolo 4, paragrafo 1, lettera c), del regolamento (UE) 2018/1725, in particolare il principio della minimizzazione dei dati, per quanto riguarda i set di dati di addestramento, convalida e prova di cui al presente regolamento, si dovrebbe tenere debitamente conto dell'intero ciclo di vita del sistema di IA.

(45) Ai fini dello sviluppo di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli dell'innovazione digitale, gli impianti di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei rispettivi settori di attività connessi al presente regolamento. Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA. Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di intelligenza artificiale su tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale. Le autorità competenti interessate, comprese quelle settoriali, che forniscono o sostengono l'accesso ai dati, possono anche sostenere la fornitura di dati di alta qualità a fini di addestramento, convalida e prova dei sistemi di IA.

(46) Disporre di informazioni sulle modalità di sviluppo dei sistemi di IA ad alto rischio e sulle loro modalità di funzionamento durante tutto il ciclo di vita è essenziale per verificare la conformità ai requisiti di cui al presente regolamento. Occorre a tal fine conservare le registrazioni e disporre di una documentazione tecnica contenente le informazioni necessarie per valutare la conformità del sistema di IA ai requisiti pertinenti. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti generali del sistema, gli algoritmi, i dati, l'addestramento, i processi di prova e di convalida utilizzati, nonché la documentazione sul pertinente sistema di gestione dei rischi. È opportuno tenere aggiornata la documentazione tecnica. Inoltre, i fornitori o gli utenti dovrebbero conservare i log generati automaticamente dal sistema di IA ad alto rischio, compresi ad esempio i dati di output, la data e l'ora di inizio, ecc., nella misura in cui tale sistema e i relativi log sono sotto il loro controllo, per un periodo adeguato a consentire loro di adempiere ai propri obblighi.

(47) Per ovviare all'opacità che può rendere alcuni sistemi di IA incomprensibili o troppo complessi per le persone fisiche, è opportuno imporre un certo grado di trasparenza per i sistemi di IA ad alto rischio. Gli utenti dovrebbero poter interpretare gli output del sistema e utilizzarlo in modo adeguato. I sistemi di IA ad alto rischio dovrebbero pertanto essere corredati di documentazione e istruzioni per l'uso pertinenti, nonché di informazioni concise e chiare, anche in relazione, se del caso, ai possibili rischi in termini di diritti fondamentali e discriminazione delle persone che possono essere interessate dal sistema alla luce della sua finalità prevista. Per facilitare la comprensione delle istruzioni per l'uso da parte degli utenti, esse dovrebbero contenere, se del caso, esempi illustrativi.

(48) I sistemi di IA ad alto rischio dovrebbero essere progettati e sviluppati in modo da consentire alle persone fisiche di sorvegliarne il funzionamento. Il fornitore del sistema dovrebbe a tal fine individuare misure di sorveglianza umana adeguate prima dell'immissione del sistema sul mercato o della sua messa in servizio. Tali misure dovrebbero in particolare garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo. Tenuto conto delle conseguenze significative per le persone in caso di corrispondenze non corrette da parte di determinati sistemi di identificazione biometrica, è opportuno prevedere un requisito rafforzato di sorveglianza umana per tali sistemi, in modo che l'utente non possa adottare alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato separatamente da almeno due persone fisiche. Tali persone potrebbero provenire da una o più entità e comprendere la persona che gestisce o utilizza il sistema. Tale requisito non dovrebbe comportare oneri o ritardi inutili e potrebbe essere sufficiente che le verifiche separate da parte delle diverse persone siano automaticamente registrate nei log generati dal sistema.

(49) Le prestazioni dei sistemi di IA ad alto rischio dovrebbero essere coerenti durante tutto il loro ciclo di vita e tali sistemi dovrebbero garantire un livello adeguato di accuratezza, robustezza e cibersicurezza, conformemente allo stato dell'arte generalmente riconosciuto. È opportuno che i livelli di precisione e le pertinenti metriche di accuratezza siano comunicati agli utenti.

(50) La robustezza tecnica è un requisito fondamentale dei sistemi di IA ad alto rischio. Essi dovrebbero essere resilienti in relazione a comportamenti dannosi o altrimenti indesiderati che possono derivare da limitazioni all'interno dei sistemi o dell'ambiente in cui i sistemi funzionano (ad esempio errori, guasti, incongruenze, situazioni impreviste). I sistemi di IA ad alto rischio dovrebbero pertanto essere progettati e sviluppati con soluzioni tecniche adeguate per prevenire o ridurre al minimo tali comportamenti dannosi o altrimenti indesiderati, come ad esempio meccanismi che consentano al sistema di interrompere in modo sicuro il proprio funzionamento ("piani fail-safe") in presenza di determinate anomalie o quando il funzionamento ha luogo al di fuori di determinati limiti prestabiliti. La mancata protezione da tali rischi potrebbe avere ripercussioni sulla sicurezza o incidere negativamente sui diritti fondamentali, ad esempio a causa della generazione da parte del sistema di IA di decisioni errate o di output sbagliati o distorti.

(51) La cibersicurezza svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza. Gli attacchi informatici contro i sistemi di IA possono far leva sulle risorse specifiche dell'IA, quali i set di dati di addestramento (ad esempio "avvelenamento dei dati", data poisoning) o i modelli addestrati (ad esempio "attacchi antagonisti", adversarial attacks), o sfruttare le vulnerabilità delle risorse digitali del sistema di IA o dell'infrastruttura TIC sottostante. Al fine di garantire un livello di cibersicurezza adeguato ai rischi, è pertanto opportuno che i fornitori di sistemi di IA ad alto rischio adottino misure adeguate, anche tenendo debitamente conto dell'infrastruttura TIC sottostante.

(52) Nell'ambito della normativa di armonizzazione dell'Unione, è opportuno che le regole applicabili all'immissione sul mercato, alla messa in servizio e all'uso di sistemi di IA ad alto rischio siano stabilite conformemente al regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[22] che pone norme in materia di accreditamento e vigilanza del mercato dei prodotti, alla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio[23] relativa a un quadro comune per la commercializzazione dei prodotti e al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio[24] sulla vigilanza del mercato e sulla conformità dei prodotti ("nuovo quadro legislativo per la commercializzazione dei prodotti").

(52 bis) In linea con i principi del nuovo quadro legislativo, è opportuno stabilire obblighi specifici per gli operatori pertinenti nella catena del valore dell'IA al fine di garantire la certezza del diritto e facilitare il rispetto del presente regolamento. In determinate situazioni tali operatori potrebbero agire contemporaneamente in più di un ruolo e dovrebbero pertanto adempiere cumulativamente tutti gli obblighi pertinenti associati a tali ruoli. Ad esempio, un operatore potrebbe agire contemporaneamente come distributore e importatore.

(53) È opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema.

---

22 Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

23 Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

24 Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1).

(54) È opportuno che il fornitore istituisca un solido sistema di gestione della qualità, garantisca l'espletamento della procedura di valutazione della conformità richiesta, rediga la documentazione pertinente e istituisca un sistema robusto per il monitoraggio successivo all'immissione sul mercato. Le autorità pubbliche che mettono in servizio sistemi di IA ad alto rischio per uso proprio possono adottare e attuare le regole per il sistema di gestione della qualità nell'ambito del sistema di gestione della qualità adottato a livello nazionale o regionale, a seconda dei casi, tenendo conto delle specificità del settore come pure delle competenze e dell'organizzazione dell'autorità pubblica in questione.

(54 bis) Al fine di garantire la certezza del diritto, è necessario chiarire che, a determinate condizioni specifiche, qualsiasi persona fisica o giuridica dovrebbe essere considerata un fornitore di un nuovo sistema di IA ad alto rischio e pertanto assumere tutti gli obblighi del caso. Ciò si verificherebbe, ad esempio, ove tale persona apponga il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, ovvero modifichi la finalità prevista di un sistema di IA non ad alto rischio già immesso sul mercato o messo in servizio in modo tale da rendere il sistema modificato un sistema di IA ad alto rischio. Tali disposizioni dovrebbero applicarsi fatte salve le disposizioni più specifiche stabilite in alcune normative settoriali del nuovo quadro legislativo con cui il presente regolamento dovrebbe applicarsi congiuntamente. Ad esempio, l'articolo 16, paragrafo 2, del regolamento (UE) 2017/745, che stabilisce che talune modifiche non dovrebbero essere considerate modifiche di un dispositivo tali da compromettere la sua conformità alle prescrizioni applicabili, dovrebbe continuare ad applicarsi ai sistemi di IA ad alto rischio che sono dispositivi medici ai sensi di tale regolamento.

(55) Qualora un sistema di IA ad alto rischio che è un componente di sicurezza di un prodotto disciplinato da una pertinente normativa settoriale del nuovo quadro legislativo non fosse immesso sul mercato o messo in servizio separatamente dal prodotto, il fabbricante del prodotto quale definito nella pertinente normativa del nuovo quadro legislativo dovrebbe adempiere gli obblighi del fornitore stabiliti nel presente regolamento e, in particolare, garantire che il sistema di IA integrato nel prodotto finale soddisfi i requisiti del presente regolamento.

(56) Al fine di consentire l'applicazione del presente regolamento e di creare condizioni di parità per gli operatori, e tenendo conto delle diverse forme di messa a disposizione di prodotti digitali, è importante garantire che, in qualsiasi circostanza, una persona stabilita nell'Unione possa fornire alle autorità tutte le informazioni necessarie sulla conformità di un sistema di IA. Pertanto, prima di mettere a disposizione i propri sistemi di IA nell'Unione, nel caso in cui non possa essere identificato un importatore, i fornitori stabiliti al di fuori dell'Unione dovrebbero nominare, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

(56 bis) Per i fornitori che non sono stabiliti nell'Unione, il rappresentante autorizzato svolge un ruolo chiave nel garantire la conformità dei sistemi di IA ad alto rischio da essi immessi sul mercato o messi in servizio nell'Unione e nel servire da referente stabilito nell'Unione. Dato tale ruolo chiave, e al fine di garantire che la responsabilità sia assunta ai fini dell'applicazione del presente regolamento, è opportuno rendere il rappresentante autorizzato responsabile in solido con il fornitore per i sistemi di IA ad alto rischio difettosi. La responsabilità del rappresentante autorizzato prevista dal presente regolamento lascia impregiudicate le disposizioni della direttiva 85/374/CEE in materia di responsabilità per danno da prodotti difettosi.

(57) [soppresso]

(58) In considerazione della natura dei sistemi di IA e dei possibili rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, anche per quanto riguarda la necessità di garantire un adeguato monitoraggio delle prestazioni di un sistema di IA in un contesto reale, è opportuno stabilire responsabilità specifiche per gli utenti. È in particolare opportuno che gli utenti usino i sistemi di IA ad alto rischio conformemente alle istruzioni per l'uso e che siano previsti alcuni altri obblighi in materia di monitoraggio del funzionamento dei sistemi di IA e conservazione delle registrazioni, a seconda dei casi. Tali obblighi dovrebbero lasciare impregiudicati altri obblighi degli utenti in relazione ai sistemi di IA ad alto rischio previsti dal diritto dell'Unione o nazionale e non dovrebbero applicarsi nel caso in cui il sistema sia utilizzato nel corso di un'attività personale non professionale.

(58 bis) È opportuno chiarire che il presente regolamento lascia impregiudicati gli obblighi dei fornitori e degli utenti dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali. È inoltre opportuno chiarire che gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione. Norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA istituiti a norma del presente regolamento dovrebbero facilitare l'effettiva attuazione e consentire l'esercizio dei diritti degli interessati e di altri mezzi di ricorso garantiti dal diritto dell'Unione in materia di protezione dei dati personali nonché degli altri diritti fondamentali.

(59) [soppresso]

(60) [soppresso]

(61) La normazione dovrebbe svolgere un ruolo fondamentale nel fornire soluzioni tecniche ai fornitori per garantire la conformità al presente regolamento, in linea con lo stato dell'arte. La conformità alle norme armonizzate quali definite nel regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio[25], le quali normalmente dovrebbero rispecchiare lo stato dell'arte, dovrebbe essere un modo per i fornitori di dimostrare la conformità ai requisiti del presente regolamento. Tuttavia, in assenza di riferimenti pertinenti a norme armonizzate, la Commissione dovrebbe poter stabilire, mediante atti di esecuzione, specifiche comuni per determinati requisiti ai sensi del presente regolamento come soluzione eccezionale di ripiego per agevolare l'obbligo del fornitore di conformarsi ai requisiti del presente regolamento, quando il processo di normazione è bloccato o quando vi sono ritardi nella definizione di una norma armonizzata appropriata. Se tale ritardo è dovuto alla complessità tecnica della norma in questione, la Commissione dovrebbe tenerne conto prima di prendere in considerazione la definizione di specifiche comuni. Un adeguato coinvolgimento delle piccole e medie imprese nell'elaborazione di norme a sostegno dell'attuazione del presente regolamento è essenziale per promuovere l'innovazione e la competitività nel settore dell'intelligenza artificiale all'interno dell'Unione. Tale coinvolgimento dovrebbe essere adeguatamente garantito conformemente agli articoli 5 e 6 del regolamento (CE) n. 1025/2012.

[25] Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

(61 bis) È opportuno che, fatto salvo l'uso di norme armonizzate e specifiche comuni, i fornitori beneficino di una presunzione di conformità al pertinente requisito relativo ai dati quando il loro sistema di IA ad alto rischio è stato addestrato e sottoposto a prova su dati che riflettono lo specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA è destinato a essere utilizzato. Analogamente, in linea con l'articolo 54, paragrafo 3, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, i sistemi di IA ad alto rischio certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema della cibersicurezza a norma di detto regolamento e i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* dovrebbero essere considerati conformi al requisito di cibersicurezza di cui al presente regolamento. Ciò lascia impregiudicata la natura volontaria di tale sistema di cibersicurezza.

(62) Al fine di garantire un elevato livello di affidabilità dei sistemi di IA ad alto rischio, è opportuno sottoporre tali sistemi a una valutazione della conformità prima della loro immissione sul mercato o messa in servizio.

(63) Al fine di ridurre al minimo l'onere per gli operatori ed evitare eventuali duplicazioni, la conformità ai requisiti del presente regolamento dei sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione secondo l'approccio del nuovo quadro legislativo dovrebbe essere valutata nell'ambito della valutazione della conformità già prevista da tale normativa. L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica specifica, la metodologia o la struttura generale della valutazione della conformità a norma della pertinente normativa specifica del nuovo quadro legislativo. Tale approccio si riflette pienamente nell'interazione tra il presente regolamento e il [regolamento macchine]. Mentre i requisiti del presente regolamento fanno fronte ai rischi per la sicurezza dei sistemi di IA che assolvono funzioni di sicurezza nelle macchine, alcuni requisiti specifici del [regolamento macchine] garantiranno l'integrazione sicura del sistema di IA nella macchina nel suo complesso, in modo da non compromettere la sicurezza di quest'ultima. Il [regolamento macchine] applica la stessa definizione di sistema di IA di cui al presente regolamento. Per quanto riguarda i sistemi di IA ad alto rischio relativi ai prodotti disciplinati dai regolamenti (UE) 745/2017 e (UE) 746/2017 relativi ai dispositivi medici, l'applicabilità dei requisiti del presente regolamento dovrebbe lasciare impregiudicata e tenere conto della logica di gestione del rischio e della valutazione del rapporto beneficio/rischio effettuata nel quadro dei dispositivi medici.

(64) In considerazione della più ampia esperienza dei certificatori professionali pre-commercializzazione nel settore della sicurezza dei prodotti e della diversa natura dei rischi connessi, è opportuno limitare, almeno in una fase iniziale di applicazione del presente regolamento, l'ambito di applicazione della valutazione della conformità da parte di terzi ai sistemi di IA ad alto rischio diversi da quelli collegati ai prodotti. È pertanto opportuno che la valutazione della conformità di tali sistemi sia di norma effettuata dal fornitore sotto la propria responsabilità, con la sola eccezione dei sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota di persone, per i quali è opportuno prevedere il coinvolgimento di un organismo notificato nella valutazione della conformità, nella misura in cui tali sistemi non siano vietati.

(65) Ai fini della valutazione della conformità da parte di terzi dei sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota delle persone, è opportuno che le autorità nazionali competenti notifichino gli organismi notificati a norma del presente regolamento, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza e assenza di conflitti di interesse. La notifica di tali organismi dovrebbe essere trasmessa dalle autorità nazionali competenti alla Commissione e agli altri Stati membri mediante lo strumento elettronico di notifica elaborato e gestito dalla Commissione a norma dell'articolo R23 della decisione 768/2008.

(66) In linea con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, è opportuno che ogniqualvolta intervenga una modifica che possa incidere sulla conformità del sistema di IA ad alto rischio al presente regolamento (per es., modifica del sistema operativo o dell'architettura del software), oppure quando viene modificata la finalità prevista del sistema, tale sistema di IA sia considerato un nuovo sistema di IA che dovrebbe essere sottoposto a una nuova valutazione della conformità. Tuttavia, le modifiche apportate all'algoritmo e alle prestazioni dei sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio (ossia adattando automaticamente le modalità di svolgimento delle funzioni) non dovrebbero costituire una modifica sostanziale, a condizione che tali modifiche siano state predeterminate dal fornitore e valutate al momento della valutazione della conformità.

(67) I sistemi di IA ad alto rischio dovrebbero recare la marcatura CE per indicare la loro conformità al presente regolamento, in modo da poter circolare liberamente nel mercato interno. Gli Stati membri non dovrebbero ostacolare in maniera ingiustificata l'immissione sul mercato o la messa in servizio di sistemi di IA ad alto rischio che soddisfano i requisiti stabiliti nel presente regolamento e recano la marcatura CE.

(68) La disponibilità in tempi rapidi di tecnologie innovative può, a determinate condizioni, essere fondamentale per la salute e la sicurezza delle persone e per la società nel suo insieme. È pertanto opportuno che, per motivi eccezionali di pubblica sicurezza o di tutela della vita e della salute delle persone fisiche nonché della proprietà industriale e commerciale, gli Stati membri possano autorizzare l'immissione sul mercato o la messa in servizio di sistemi di IA che non sono stati sottoposti a una valutazione della conformità.

(69) Al fine di agevolare il lavoro della Commissione e degli Stati membri nel settore dell'intelligenza artificiale e di aumentare la trasparenza nei confronti del pubblico, è opportuno che i fornitori di sistemi di IA ad alto rischio diversi da quelli collegati a prodotti che rientrano nell'ambito di applicazione della pertinente normativa di armonizzazione dell'Unione vigente siano tenuti a registrarsi e a registrare informazioni sul loro sistema di IA ad alto rischio in una banca dati dell'UE, che sarà istituita e gestita dalla Commissione. Prima di utilizzare un sistema di IA ad alto rischio elencato nell'allegato III, anche gli utenti di sistemi di IA ad alto rischio che sono autorità, agenzie od organismi pubblici, ad eccezione delle autorità di contrasto, delle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo, e le autorità che sono utenti di sistemi di IA ad alto rischio nel settore delle infrastrutture critiche si registrano in tale banca dati e selezionano il sistema che intendono utilizzare. È opportuno che la Commissione sia la titolare del trattamento di tale banca dati conformemente al regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[26]. Al fine di garantire la piena funzionalità della banca dati, è opportuno che, al momento dell'attivazione, la procedura per l'istituzione della banca dati preveda l'elaborazione di specifiche funzionali da parte della Commissione e una relazione di audit indipendente.

[26] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

(70) Alcuni sistemi di IA destinati all'interazione con persone fisiche o alla generazione di contenuti possono comportare rischi specifici di impersonificazione o inganno, a prescindere dal fatto che siano considerati ad alto rischio o no. L'uso di tali sistemi dovrebbe pertanto essere, in determinate circostanze, soggetto a specifici obblighi di trasparenza, fatti salvi i requisiti e gli obblighi per i sistemi di IA ad alto rischio. Le persone fisiche dovrebbero in particolare ricevere una notifica nel momento in cui interagiscono con un sistema di IA, a meno che tale interazione 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. Nell'attuare tale obbligo, le caratteristiche delle persone appartenenti a gruppi vulnerabili a causa della loro età o disabilità dovrebbero essere prese in considerazione nella misura in cui il sistema di IA sia destinato a interagire anche con tali gruppi. È inoltre opportuno che le persone fisiche ricevano una notifica quando sono esposte a sistemi che, nel trattamento dei loro dati biometrici, possono identificare o dedurre le emozioni o intenzioni di tali persone e assegnarle a categorie specifiche. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti personali, l'origine etnica, le preferenze e gli interessi personali o altri aspetti quali l'orientamento sessuale o politico. Tali informazioni e notifiche dovrebbero essere fornite in formati accessibili alle persone con disabilità. Inoltre, gli utenti che utilizzano un sistema di IA per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a persone, luoghi o eventi esistenti e che potrebbero apparire falsamente autentici, dovrebbero rendere noto che il contenuto è stato creato o manipolato artificialmente etichettando come tali gli output dell'intelligenza artificiale e rivelandone l'origine artificiale. La conformità agli obblighi di informazione di cui sopra non dovrebbe essere interpretata nel senso che l'uso del sistema o dei suoi output è lecito ai sensi del presente regolamento o di altre normative dell'Unione e degli Stati membri e dovrebbe lasciare impregiudicati gli altri obblighi di trasparenza per gli utenti dei sistemi di IA stabiliti dal diritto dell'Unione o nazionale. Inoltre, non dovrebbe essere interpretato nel senso che l'uso del sistema o dei suoi output ostacola il diritto alla libertà di espressione e il diritto alla libertà delle arti e delle scienze garantito dalla Carta dei diritti fondamentali dell'UE, in particolare quando il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico o fittizio, fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

(71) L'intelligenza artificiale è una famiglia di tecnologie in rapida evoluzione che richiede nuove forme di sorveglianza regolamentare e uno spazio sicuro per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi. Al fine di garantire un quadro giuridico favorevole all'innovazione, adeguato alle esigenze future e resiliente alle perturbazioni, è opportuno incoraggiare le autorità nazionali competenti di uno o più Stati membri a istituire spazi di sperimentazione normativa in materia di intelligenza artificiale per agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio.

(72) Gli obiettivi degli spazi di sperimentazione normativa per l'IA dovrebbero essere la promozione dell'innovazione in materia di IA, mediante la creazione di un ambiente controllato di sperimentazione e prova nella fase di sviluppo e pre-commercializzazione al fine di garantire la conformità dei sistemi di IA innovativi al presente regolamento e ad altre normative pertinenti dell'Unione e degli Stati membri, e il rafforzamento della certezza del diritto per gli innovatori e della sorveglianza e della comprensione da parte delle autorità competenti delle opportunità, dei rischi emergenti e degli impatti dell'uso dell'IA, nonché l'accelerazione dell'accesso ai mercati, anche mediante l'eliminazione degli ostacoli per le piccole e medie imprese (PMI), comprese le start-up. La partecipazione allo spazio di sperimentazione normativa per l'IA dovrebbe concentrarsi su questioni che creano incertezza giuridica rendendo difficoltoso per i fornitori e i potenziali fornitori innovare, sperimentare l'IA nell'Unione e contribuire all'apprendimento normativo basato su dati concreti. La supervisione dei sistemi di IA nello spazio di sperimentazione normativa per l'IA dovrebbe pertanto riguardare il relativo sviluppo, addestramento, prova e convalida prima che i sistemi siano immessi sul mercato o messi in servizio, nonché la nozione e il verificarsi di modifiche sostanziali che possono richiedere una nuova procedura di valutazione della conformità. Se del caso, le autorità nazionali competenti che istituiscono spazi di sperimentazione normativa per l'IA dovrebbero cooperare con altre autorità pertinenti, comprese quelle che vigilano sulla protezione dei diritti fondamentali, e potrebbero consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA, quali organizzazioni di normazione nazionali o europee, organismi notificati, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione, poli di innovazione e pertinenti portatori di interessi e organizzazioni della società civile. Al fine di garantire un'attuazione uniforme in tutta l'Unione ed economie di scala, è opportuno stabilire regole comuni per l'attuazione degli spazi di sperimentazione normativa e un quadro per la cooperazione tra le autorità competenti coinvolte nel controllo degli spazi di sperimentazione. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del presente regolamento non dovrebbero pregiudicare altre normative che consentono la creazione di altri spazi di sperimentazione volti a garantire la conformità alla legislazione diversa dal presente regolamento. Se del caso, le pertinenti autorità competenti responsabili di tali altri spazi di sperimentazione normativa dovrebbero considerare i vantaggi derivanti dall'utilizzo di tali spazi di sperimentazione anche al fine di garantire la conformità dei sistemi di IA al presente regolamento. Previo accordo tra le autorità nazionali competenti e i partecipanti allo spazio di sperimentazione normativa per l'IA, anche le prove in condizioni reali possono essere gestite e supervisionate nel quadro dello spazio di sperimentazione normativa per l'IA.

(-72 bis) Il presente regolamento dovrebbe fornire la base giuridica ai partecipanti allo spazio di sperimentazione normativa per l'IA per utilizzare i dati personali raccolti per altre finalità ai fini dello sviluppo di determinati sistemi di IA di interesse pubblico nell'ambito dello spazio di sperimentazione normativa per l'IA, in linea con l'articolo 6, paragrafo 4, e l'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679, e con gli articoli 5 e 10 del regolamento (UE) 2018/1725, e fatti salvi l'articolo 4, paragrafo 2, e l'articolo 10 della direttiva (UE) 2016/680. Tutti gli altri obblighi dei titolari del trattamento e i diritti degli interessati ai sensi del regolamento (UE) 2016/679, del regolamento (UE) 2018/1725 e della direttiva (UE) 2016/680 restano applicabili. In particolare, il presente regolamento non dovrebbe costituire una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b), del regolamento (UE) 2016/679 e dell'articolo 24, paragrafo 2, lettera b), del regolamento (UE) 2018/1725. I partecipanti allo spazio di sperimentazione dovrebbero fornire garanzie adeguate e cooperare con le autorità competenti, anche seguendo i loro orientamenti e agendo rapidamente e in buona fede per attenuare eventuali rischi elevati per la sicurezza e i diritti fondamentali che possono emergere durante lo sviluppo e la sperimentazione nello spazio sopraindicato. È opportuno che le autorità competenti, nel decidere se infliggere una sanzione amministrativa pecuniaria a norma dell'articolo 83, paragrafo 2, del regolamento 2016/679 e dell'articolo 57 della direttiva 2016/680, tengano conto della condotta dei partecipanti allo spazio di sperimentazione.

(72 bis) Al fine di accelerare il processo di sviluppo e immissione sul mercato dei sistemi di IA ad alto rischio elencati nell'allegato III, è importante che anche i fornitori o i potenziali fornitori di tali sistemi possano beneficiare di un regime specifico per sottoporre a prova tali sistemi in condizioni reali, senza partecipare a uno spazio di sperimentazione normativa per l'IA. Tuttavia, in tali casi e tenendo conto delle possibili conseguenze di tali prove sulle persone, è opportuno garantire che il regolamento introduca garanzie e condizioni adeguate e sufficienti per i fornitori o potenziali fornitori. Tali garanzie dovrebbero includere, tra l'altro, la richiesta del consenso informato delle persone fisiche a partecipare a prove in condizioni reali, ad eccezione delle autorità di contrasto nei casi in cui la richiesta di consenso informato impedirebbe che il sistema di IA sia sottoposto a prova. Il consenso dei soggetti a partecipare a tali prove a norma del presente regolamento è distinto e non pregiudica il consenso degli interessati al trattamento dei loro dati personali ai sensi della pertinente normativa in materia di protezione dei dati.

(73) Al fine di promuovere e proteggere l'innovazione, è importante che siano tenuti in particolare considerazione gli interessi delle PMI fornitrici e degli utenti di sistemi di IA. È a tal fine opportuno che gli Stati membri sviluppino iniziative destinate a tali operatori, anche in materia di sensibilizzazione e comunicazione delle informazioni. È inoltre opportuno che gli organismi notificati, nel fissare le tariffe per la valutazione della conformità, tengano in considerazione gli interessi e le esigenze specifici delle PMI fornitrici. Le spese di traduzione connesse alla documentazione obbligatoria e alla comunicazione con le autorità possono rappresentare un costo significativo per i fornitori e gli altri operatori, in particolare quelli di dimensioni ridotte. Gli Stati membri dovrebbero garantire, se possibile, che una delle lingue da essi indicate e accettate per la documentazione dei fornitori pertinenti e per la comunicazione con gli operatori sia una lingua ampiamente compresa dal maggior numero possibile di utenti transfrontalieri.

(73 bis) Al fine di promuovere e proteggere l'innovazione, la piattaforma di IA on demand e tutti i pertinenti programmi e progetti di finanziamento dell'UE, quali il programma Europa digitale e Orizzonte Europa, attuati dalla Commissione e dagli Stati membri a livello nazionale o dell'UE, dovrebbero contribuire al conseguimento degli obiettivi del presente regolamento.

(74) In particolare, al fine di ridurre al minimo i rischi per l'attuazione derivanti dalla mancanza di conoscenze e competenze sul mercato, nonché per agevolare il rispetto, da parte dei fornitori, segnatamente le PMI, e degli organismi notificati, degli obblighi loro imposti dal presente regolamento, è opportuno che la piattaforma di IA on demand, i poli europei dell'innovazione digitale e gli impianti di prova e sperimentazione istituiti dalla Commissione e dagli Stati membri a livello nazionale o dell'UE contribuiscano, se possibile, all'attuazione del presente regolamento. Nell'ambito delle rispettive missioni e dei rispettivi settori di competenza essi possono fornire, in particolare, sostegno tecnico e scientifico ai fornitori e agli organismi notificati.

(74 bis) Inoltre, al fine di garantire la proporzionalità, tenuto conto delle dimensioni molto ridotte di alcuni operatori rispetto ai costi dell'innovazione, è opportuno esentare le microimprese dagli obblighi più dispendiosi, come l'istituzione di un sistema di gestione della qualità, in modo da ridurre gli oneri amministrativi e i costi a carico di tali imprese, senza incidere sul livello di protezione e sulla necessità di rispettare i requisiti per i sistemi di IA ad alto rischio.

(75) È opportuno che la Commissione agevoli, nella misura del possibile, l'accesso agli impianti di prova e sperimentazione di organismi, gruppi o laboratori istituiti o accreditati a norma di qualsiasi pertinente normativa di armonizzazione dell'Unione che assolvano compiti nel contesto della valutazione della conformità di prodotti o dispositivi contemplati da tale normativa di armonizzazione dell'Unione. Ciò vale in particolare per i gruppi di esperti, i laboratori specializzati e i laboratori di riferimento nel settore dei dispositivi medici a norma del regolamento (UE) 2017/745 e del regolamento (UE) 2017/746.

(76) Al fine di facilitare un'attuazione agevole, efficace e armonizzata del presente regolamento, è opportuno istituire un comitato europeo per l'intelligenza artificiale. Il comitato dovrebbe riflettere i vari interessi dell'ecosistema dell'IA ed essere composto da rappresentanti degli Stati membri. Per garantire il coinvolgimento dei pertinenti portatori di interessi, è opportuno creare un sottogruppo permanente del comitato. Il comitato dovrebbe essere responsabile di una serie di compiti consultivi, tra cui l'emanazione di pareri, raccomandazioni, consulenze o il contributo all'emanazione di orientamenti su questioni relative all'attuazione del presente regolamento, comprese le questioni relative all'esecuzione, le specifiche tecniche o le norme esistenti per quanto riguarda i requisiti stabiliti nel presente regolamento, e la fornitura di consulenza alla Commissione, agli Stati membri e alle rispettive autorità nazionali competenti su questioni specifiche connesse all'intelligenza artificiale. Per offrire una certa flessibilità agli Stati membri nella designazione dei loro rappresentanti all'interno del comitato per l'IA, tali rappresentanti possono essere persone appartenenti a entità pubbliche dotate delle competenze e dei poteri pertinenti per facilitare il coordinamento a livello nazionale e contribuire all'adempimento dei compiti del comitato. Il comitato dovrebbe istituire due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e le autorità di notifica su questioni relative rispettivamente alla vigilanza del mercato e agli organismi notificati. Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per il presente regolamento ai sensi dell'articolo 30 del regolamento (UE) 2019/1020. In linea con il ruolo e i compiti della Commissione a norma dell'articolo 33 del regolamento (UE) 2019/1020, la Commissione dovrebbe sostenere le attività del sottogruppo permanente per la vigilanza del mercato effettuando valutazioni o studi di mercato, in particolare al fine di individuare gli aspetti del presente regolamento che richiedono un coordinamento specifico e urgente tra le autorità di vigilanza del mercato. Il comitato può istituire altri sottogruppi permanenti o temporanei, ove opportuno, ai fini dell'esame di questioni specifiche. Il comitato dovrebbe inoltre cooperare, se del caso, con i pertinenti organismi, gruppi di esperti e reti dell'UE attivi nel contesto della legislazione dell'UE interessata, compresi in particolare quelli attivi a norma del pertinente regolamento dell'UE sui dati, i prodotti e i servizi digitali.

(76 bis) La Commissione dovrebbe sostenere attivamente gli Stati membri e gli operatori nell'attuazione e nell'esecuzione del presente regolamento. A tale riguardo, dovrebbe elaborare orientamenti su temi specifici volti a facilitare l'applicazione del presente regolamento, prestando nel contempo particolare attenzione alle esigenze delle PMI e delle start-up nei settori con maggiore probabilità di essere interessati. Al fine di sostenere un'esecuzione adeguata e le capacità degli Stati membri, è opportuno istituire e mettere a disposizione degli Stati membri impianti di prova dell'Unione sull'IA e un gruppo di esperti pertinenti.

(77) Gli Stati membri svolgono un ruolo chiave nell'applicare il presente regolamento e nel garantirne il rispetto. A tale riguardo, è opportuno che ciascuno Stato membro designi una o più autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del presente regolamento. Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica per svolgere i compiti delle autorità nazionali competenti ai sensi del presente regolamento, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali.

(78) Al fine di garantire che i fornitori di sistemi di IA ad alto rischio possano tenere in considerazione l'esperienza sull'uso di sistemi di IA ad alto rischio per migliorare i loro sistemi e il processo di progettazione e sviluppo o possano adottare tempestivamente eventuali misure correttive, è opportuno che tutti i fornitori dispongano di un sistema di monitoraggio successivo all'immissione sul mercato. Tale sistema è altresì fondamentale per garantire che i possibili rischi derivanti dai sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio possano essere affrontati in modo più efficiente e tempestivo. I fornitori dovrebbero anche essere tenuti, in tale contesto, a predisporre un sistema per segnalare alle autorità competenti eventuali incidenti gravi derivanti dall'uso dei loro sistemi di IA.

(79) Al fine di garantire un'applicazione adeguata ed efficace dei requisiti e degli obblighi stabiliti dal presente regolamento, che costituisce la normativa di armonizzazione dell'Unione, è opportuno che si applichi nella sua interezza il sistema di vigilanza del mercato e di conformità dei prodotti istituito dal regolamento (UE) 2019/1020. Le autorità di vigilanza del mercato designate a norma del presente regolamento dovrebbero disporre di tutti i poteri di esecuzione ai sensi del presente regolamento e del regolamento (UE) 2019/1020 e dovrebbero esercitare i loro poteri e svolgere le loro funzioni in modo indipendente, imparziale e senza pregiudizi. Sebbene la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici a norma del presente regolamento, le autorità di vigilanza del mercato possono adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conformemente al presente regolamento. Data la natura specifica delle istituzioni, degli organi e degli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento, è opportuno designare il Garante europeo della protezione dei dati quale autorità di vigilanza del mercato per essi competente. Ciò non dovrebbe pregiudicare la designazione di autorità nazionali competenti da parte degli Stati membri. Le attività di vigilanza del mercato non dovrebbero pregiudicare la capacità delle entità sottoposte a vigilanza di svolgere i loro compiti in modo indipendente, qualora tale indipendenza sia richiesta dal diritto dell'Unione.

(79 bis) Il presente regolamento non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione della normativa dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati. Ove necessario per il loro mandato, è opportuno che tali autorità od organismi pubblici nazionali abbiano altresì accesso alla documentazione creata a norma del presente regolamento. È opportuno istituire una procedura di salvaguardia specifica per garantire un'applicazione adeguata e tempestiva rispetto ai sistemi di IA che presentano un rischio per la salute, la sicurezza e i diritti fondamentali. La procedura per siffatti sistemi di IA che presentano un rischio dovrebbe essere applicata ai sistemi di IA ad alto rischio che presentano un rischio, ai sistemi vietati che sono stati immessi sul mercato, messi in servizio o utilizzati in violazione delle pratiche vietate di cui al presente regolamento e ai sistemi di IA che sono stati messi a disposizione in violazione dei requisiti di trasparenza di cui al presente regolamento e che presentano un rischio.

(80) La legislazione dell'Unione in materia di servizi finanziari comprende regole e requisiti in materia di governance interna e di gestione dei rischi che sono applicabili agli istituti finanziari regolamentati durante la fornitura di tali servizi, anche quando si avvalgono di sistemi di IA. Al fine di garantire la coerenza dell'applicazione e dell'attuazione degli obblighi previsti dal presente regolamento e delle regole e dei requisiti pertinenti della normativa dell'Unione in materia di servizi finanziari, è opportuno che le autorità responsabili del controllo e dell'applicazione della normativa in materia di servizi finanziari siano designate come autorità competenti ai fini del controllo dell'attuazione del presente regolamento, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza, a meno che gli Stati membri non decidano di designare un'altra autorità per svolgere tali compiti di vigilanza del mercato. Tali autorità competenti dovrebbero disporre di tutti i poteri a norma del presente regolamento e del regolamento (UE) 2019/1020 sulla vigilanza del mercato per far rispettare i requisiti e gli obblighi del presente regolamento, compresi i poteri per svolgere attività di vigilanza del mercato ex post che possono essere integrate, se del caso, nei rispettivi meccanismi e nelle rispettive procedure di vigilanza esistenti a norma della pertinente normativa dell'Unione in materia di servizi finanziari. È opportuno prevedere che, quando agiscono in qualità di autorità di vigilanza del mercato a norma del presente regolamento, le autorità nazionali responsabili della vigilanza degli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento n. 1024/2013 del Consiglio, comunichino senza ritardo alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento. Per migliorare ulteriormente la coerenza tra il presente regolamento e le regole applicabili agli enti creditizi disciplinati dalla direttiva 2013/36/UE del Parlamento europeo e del Consiglio[27], è altresì opportuno integrare negli obblighi e nelle procedure esistenti a norma di tale direttiva alcuni degli obblighi procedurali dei fornitori in materia di gestione dei rischi, monitoraggio successivo alla commercializzazione e documentazione. Al fine di evitare sovrapposizioni, è opportuno prevedere deroghe limitate anche in relazione al sistema di gestione della qualità dei fornitori e all'obbligo di monitoraggio imposto agli utenti dei sistemi di IA ad alto rischio nella misura in cui si applicano agli enti creditizi disciplinati dalla direttiva 2013/36/UE. Lo stesso regime dovrebbe applicarsi alle imprese di assicurazione e di riassicurazione e alle società di partecipazione assicurativa ai sensi della

[27] Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

direttiva 2009/138/UE (Solvibilità II) nonché agli intermediari assicurativi ai sensi della direttiva (UE) 2016/97 e ad altri tipi di istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della pertinente normativa dell'Unione sui servizi finanziari per garantire coerenza e parità di trattamento nel settore finanziario.

(81) Lo sviluppo di sistemi di IA diversi dai sistemi di IA ad alto rischio in conformità ai requisiti del presente regolamento può portare a una più ampia adozione nell'Unione dell'intelligenza artificiale affidabile. I fornitori di sistemi di IA non ad alto rischio dovrebbero essere incoraggiati a creare codici di condotta volti a promuovere l'applicazione volontaria dei requisiti applicabili ai sistemi di IA ad alto rischio, adattati in funzione della finalità prevista dei sistemi e del minor rischio connesso. I fornitori dovrebbero inoltre essere incoraggiati ad applicare su base volontaria requisiti supplementari relativi, ad esempio, alla sostenibilità ambientale, all'accessibilità per le persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo di sistemi di IA e alla diversità dei gruppi che si occupano dello sviluppo. La Commissione può elaborare iniziative, anche di natura settoriale, per agevolare la riduzione degli ostacoli tecnici che ostruiscono lo scambio transfrontaliero di dati per lo sviluppo dell'IA, anche per quanto riguarda l'infrastruttura di accesso ai dati e l'interoperabilità semantica e tecnica dei diversi tipi di dati.

(82) È importante che i sistemi di IA collegati a prodotti che non sono ad alto rischio in conformità al presente regolamento e che pertanto non sono tenuti a rispettare i requisiti ivi stabiliti siano comunque sicuri al momento dell'immissione sul mercato o della messa in servizio. Per contribuire a tale obiettivo, sarebbe opportuno applicare come rete di sicurezza la direttiva 2001/95/CE del Parlamento europeo e del Consiglio[28].

(83) Al fine di garantire una cooperazione affidabile e costruttiva delle autorità competenti a livello nazionale e dell'Unione, è opportuno che tutte le parti coinvolte nell'applicazione del presente regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nell'assolvimento dei loro compiti, in conformità del diritto dell'Unione o nazionale.

[28] Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti (GU L 11 del 15.1.2002, pag. 4).

(84) Gli Stati membri dovrebbero adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni di cui al presente regolamento, anche stabilendo sanzioni effettive, proporzionate e dissuasive in caso di violazione e nel rispetto del principio *ne bis in idem*. Per talune violazioni specifiche, è opportuno che gli Stati membri tengano conto dei margini e dei criteri stabiliti nel presente regolamento. Il Garante europeo della protezione dei dati dovrebbe disporre del potere di infliggere sanzioni pecuniarie alle istituzioni, agli organi e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento.

(85) Al fine di garantire che il quadro normativo possa essere adeguato ove necessario, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per modificare la normativa di armonizzazione dell'Unione elencata nell'allegato II, i sistemi di IA ad alto rischio elencati nell'allegato III, le disposizioni relative alla documentazione tecnica di cui all'allegato IV, il contenuto della dichiarazione di conformità UE di cui all'allegato V, le disposizioni relative alle procedure di valutazione della conformità di cui agli allegati VI e VII e le disposizioni che stabiliscono i sistemi di IA ad alto rischio cui dovrebbe applicarsi la procedura di valutazione della conformità sulla base della valutazione del sistema di gestione della qualità e della valutazione della documentazione tecnica. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[29]. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati. Tali consultazioni e consulenze dovrebbero essere altresì svolte nel quadro delle attività del comitato per l'IA e dei suoi sottogruppi.

[29] GU L 123 del 12.5.2016, pag. 1.

(86) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione del presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[30]. È di particolare importanza che, conformemente ai principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016, qualora siano necessarie cognizioni più ampie in una fase precoce dell'elaborazione di un progetto di atto di esecuzione, la Commissione si rivolga a gruppi di esperti, consulti specifici portatori di interessi o effettui consultazioni pubbliche, a seconda dei casi. Tali consultazioni e consulenze dovrebbero essere altresì svolte nel quadro delle attività del comitato per l'IA e dei suoi sottogruppi, anche per quanto riguarda la preparazione di atti di esecuzione in relazione agli articoli 4, 4 ter e 6.

(87) Poiché l'obiettivo del presente regolamento non può essere conseguito in misura sufficiente dagli Stati membri e, a motivo della portata o degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 TUE. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(87 bis) Al fine di garantire la certezza del diritto, assicurare un adeguato periodo di adattamento per gli operatori ed evitare perturbazioni del mercato, anche garantendo la continuità dell'uso dei sistemi di IA, è opportuno che il presente regolamento si applichi ai sistemi di IA ad alto rischio che sono stati immessi sul mercato o messi in servizio prima della data generale di applicazione dello stesso, solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione o finalità prevista. È opportuno precisare che, a tale riguardo, il concetto di modifica significativa dovrebbe essere inteso come equivalente nella sostanza alla nozione di modifica sostanziale, utilizzata solo per i sistemi di IA ad alto rischio quali definiti nel presente regolamento.

---

[30] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

(88) Il presente regolamento dovrebbe applicarsi a decorrere dal... [*OP: inserire la data stabilita all'articolo 85*]. È tuttavia opportuno che l'infrastruttura relativa alla governance e al sistema di valutazione della conformità sia operativa prima di tale data, pertanto le disposizioni sugli organismi notificati e sulla struttura di governance dovrebbero applicarsi a decorrere dal... [*OP: inserire la data corrispondente a tre mesi dopo l'entrata in vigore del presente regolamento*]. Gli Stati membri dovrebbero inoltre stabilire e notificare alla Commissione la normativa relativa alle sanzioni, comprese le sanzioni amministrative pecuniarie, e garantire che essa sia attuata in modo corretto ed efficace entro la data di applicazione del presente regolamento. Le disposizioni relative alle sanzioni dovrebbero pertanto applicarsi a decorrere dal [*OP: inserire la data corrispondente a dodici mesi dopo l'entrata in vigore del presente regolamento*].

(89) Conformemente all'articolo 42, paragrafo 2, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati e hanno formulato il loro parere il [...],

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

TITOLO I

DISPOSIZIONI GENERALI

Articolo 1
Oggetto

Il presente regolamento stabilisce:

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

a) il divieto di determinate pratiche di intelligenza artificiale;

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

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

d) regole in materia di monitoraggio del mercato, vigilanza del mercato e governance;

e) misure a sostegno dell'innovazione.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica:

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

b) agli utenti dei sistemi di IA che sono fisicamente presenti o stabiliti nell'Unione;

c) ai fornitori e agli utenti di sistemi di IA che sono fisicamente presenti o stabiliti in un paese terzo, laddove l'output prodotto dal sistema 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, stabiliti nell'Unione;

2. Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafi 1 e 2, relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione di cui all'allegato II, sezione B, si applica unicamente l'articolo 84 del presente regolamento. L'articolo 53 si applica solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati nel quadro di tale normativa di armonizzazione dell'Unione.

3. 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 modifica di tali sistemi ai fini di attività che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, di attività riguardanti le forze armate, la difesa o la sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

   Inoltre, 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 ai fini di attività che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, di attività riguardanti le forze armate, la difesa o la 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 di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri.

5. Il presente regolamento non pregiudica l'applicazione delle disposizioni sulla responsabilità dei prestatori intermediari di cui al capo II, sezione 4, della direttiva 2000/31/CE del Parlamento europeo e del Consiglio[31] [*da sostituire con le corrispondenti disposizioni della legge sui servizi digitali*].

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

7. Il presente regolamento non si applica alle attività di ricerca e sviluppo relative ai sistemi di IA.

8. Il presente regolamento non si applica agli obblighi degli utenti che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale, ad eccezione dell'articolo 52.

---

[31] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") (GU L 178 del 17.7.2000, pag. 1).

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) "sistema di intelligenza artificiale" (sistema di IA): un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativi), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce;

1 bis) "ciclo di vita di un sistema di IA": la durata di un sistema di IA, dalla progettazione fino alla dismissione. Fatti salvi i poteri delle autorità di vigilanza del mercato, tale dismissione può avvenire in qualsiasi momento durante la fase di monitoraggio successivo all'immissione sul mercato su decisione del fornitore e implica che il sistema non possa essere utilizzato ulteriormente. Il ciclo di vita di un sistema di IA si conclude anche con una modifica sostanziale del sistema di IA apportata dal fornitore o da qualsiasi altra persona fisica o giuridica, nel qual caso il sistema di IA modificato in modo sostanziale è considerato un nuovo sistema di IA;

1 ter) "sistema di IA per finalità generali": un sistema di IA che, indipendentemente dalla modalità con cui è immesso sul mercato o messo in servizio, anche come software open source, è destinato secondo le intenzioni del fornitore a svolgere funzioni di applicazione generale quali il riconoscimento di immagini o vocale, la creazione di audio o video, la rilevazione di modelli, la risposta a domande, la traduzione o altro; un sistema di IA per finalità generali può essere utilizzato in una varietà di contesti e può essere integrato in una varietà di altri sistemi di IA;

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

3) [soppresso];

3 bis) "piccole e medie imprese" (PMI): un'impresa quale definita nell'allegato della raccomandazione 2003/361/CE della Commissione relativa alla definizione delle microimprese, piccole e medie imprese;

4) "utente": qualsiasi persona fisica o giuridica, compresa un'autorità pubblica, un'agenzia o altro organismo, sotto la cui autorità è utilizzato il sistema;

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

5 bis) "fabbricante del prodotto": un fabbricante ai sensi di uno qualsiasi degli atti della normativa di armonizzazione dell'Unione di cui all'allegato II;

6) "importatore": qualsiasi persona fisica o giuridica fisicamente presente 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 al di fuori dell'Unione;

7) "distributore": qualsiasi 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": il fornitore, il fabbricante del prodotto, l'utente, il rappresentante autorizzato, l'importatore o il distributore;

9) "immissione sul mercato": la prima messa a disposizione di un sistema di IA sul mercato dell'Unione;

10) "messa a disposizione sul mercato": qualsiasi fornitura di un sistema di IA 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 all'utente 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 ragionevolmente prevedibile;

14) "componente di sicurezza di un prodotto o di un sistema": un componente di un prodotto o di un sistema che svolge una funzione di sicurezza per tale prodotto o sistema o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni;

15) "istruzioni per l'uso": le informazioni comunicate dal fornitore per informare l'utente 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 degli utenti;

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) "valutazione della conformità": la procedura atta a verificare se i requisiti di cui al titolo III, capo 2, del presente regolamento relativi a un sistema di IA ad alto rischio sono stati soddisfatti;

20) "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;

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 designato in conformità al presente regolamento e ad altre pertinenti normative di armonizzazione dell'Unione;

23) "modifica sostanziale": una modifica del sistema di IA a seguito della sua immissione sul mercato o messa in servizio che incide sulla conformità del sistema di IA ai requisiti di cui al titolo III, capo 2, del presente regolamento o una modifica della finalità prevista per la quale il sistema di IA è stato valutato. 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;

24) "marcatura CE di conformità" (marcatura CE): una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al titolo III, capo 2, o all'articolo 4 ter del presente regolamento e in altri atti normativi applicabili dell'Unione che armonizzano le condizioni per la commercializzazione dei prodotti ("normativa di armonizzazione dell'Unione") 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 europea 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 di evitare l'eccessivo adattamento ai dati di addestramento (overfitting), considerando che il set di dati di convalida può essere un set di dati distinto o essere costituito da una partizione fissa o variabile del set di dati di addestramento;

31) "dati di prova": i dati utilizzati per fornire una valutazione indipendente del sistema di IA addestrato e convalidato al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;

32) "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;

33) "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali l'immagine facciale o i dati dattiloscopici;

34) "sistema di riconoscimento delle emozioni": un sistema di IA finalizzato all'identificazione o alla deduzione di stati psicologici, emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;

35) "sistema di categorizzazione biometrica": un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche;

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

37) "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 istantaneamente o quasi istantaneamente;

38) [soppresso]

39) "spazio accessibile al pubblico": qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che siano state prestabilite determinate condizioni o circostanze di accesso e indipendentemente dalle potenziali restrizioni di capacità;

40) "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;

41) "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;

42) [soppresso]

43) "autorità nazionale competente": l'autorità di notifica o l'autorità di vigilanza del mercato. Per quanto riguarda i sistemi di IA messi in servizio o utilizzati dalle istituzioni, dagli organi e dagli organismi dell'UE, il Garante europeo della protezione dei dati assolve le responsabilità che negli Stati membri sono attribuite all'autorità nazionale competente e, se del caso, qualsiasi riferimento alle autorità nazionali competenti o alle autorità di vigilanza del mercato nel presente regolamento si intende fatto al Garante europeo della protezione dei dati;

44) "incidente grave": qualsiasi incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, causa una delle seguenti conseguenze:

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

b) una perturbazione grave e irreversibile della gestione e 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;

45) "infrastruttura critica": un elemento, un sistema o parte di questo, necessario per la prestazione di un servizio essenziale per il mantenimento di funzioni vitali della società o di attività economiche ai sensi dell'articolo 2, paragrafi 4 e 5, della direttiva …../….. sulla resilienza dei soggetti critici;

46) "dati personali": dati quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;

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

48) "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; la prova in condizioni reali 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 53 o all'articolo 54 bis;

49) "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;

50) "soggetto": ai fini della prova in condizioni reali, una persona fisica che partecipa a prove in condizioni reali;

51) "consenso informato": l'espressione libera 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; nel caso di minori e di soggetti incapaci, il consenso informato è fornito dal rispettivo rappresentante legalmente designato;

52) "spazio di sperimentazione normativa per l'IA": un quadro concreto istituito da un'autorità nazionale 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 specifico per un periodo di tempo limitato sotto supervisione regolamentare.

Articolo 4

Atti di esecuzione

Al fine di garantire condizioni uniformi di esecuzione del presente regolamento per quanto riguarda gli approcci di apprendimento automatico e gli approcci basati sulla logica e sulla conoscenza di cui all'articolo 3, punto 1, la Commissione può adottare atti di esecuzione per specificare gli elementi tecnici di tali approcci, tenendo conto degli sviluppi tecnologici e di mercato. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

TITOLO I BIS

SISTEMI DI IA PER FINALITÀ GENERALI

Articolo 4 bis

Conformità dei sistemi di IA per finalità generali al presente regolamento

1. Fatti salvi gli articoli 5, 52, 53 e 69 del presente regolamento, i sistemi di IA per finalità generali rispettano unicamente i requisiti e gli obblighi di cui all'articolo 4 ter.

2. Tali requisiti e obblighi si applicano indipendentemente dal fatto che il sistema di IA per finalità generali sia immesso sul mercato o messo in servizio come modello preaddestrato e che l'ulteriore perfezionamento del modello debba essere effettuato dall'utente del sistema di IA per finalità generali.

Articolo 4 ter

Requisiti per i sistemi di IA per finalità generali e obblighi per i fornitori di tali sistemi

1. I sistemi di IA per finalità generali che possono essere utilizzati come sistemi di IA ad alto rischio o come componenti di sistemi di IA ad alto rischio ai sensi dell'articolo 6 soddisfano i requisiti di cui al titolo III, capo 2, del presente regolamento a decorrere dalla data di applicazione degli atti di esecuzione adottati dalla Commissione secondo la procedura d'esame di cui all'articolo 74, paragrafo 2, entro 18 mesi dall'entrata in vigore del presente regolamento. Tali atti di esecuzione specificano e adattano l'applicazione dei requisiti stabiliti al titolo III, capo 2, ai sistemi di IA per finalità generali alla luce delle loro caratteristiche, della fattibilità tecnica, delle specificità della catena del valore dell'IA e degli sviluppi tecnologici e di mercato. Nel soddisfare tali requisiti, si tiene conto dello stato dell'arte generalmente riconosciuto.

2. I fornitori di sistemi di IA per finalità generali di cui al paragrafo 1 rispettano, a decorrere dalla data di applicazione degli atti di esecuzione di cui al paragrafo 1, gli obblighi di cui agli articoli 16 bis bis, 16 sexies, 16 septies, 16 octies, 16 decies, 16 undecies, 25, 48 e 61.

3. Ai fini del rispetto degli obblighi di cui all'articolo 16 sexies, i fornitori seguono la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI, punti 3 e 4.

4. I fornitori di tali sistemi tengono inoltre la documentazione tecnica di cui all'articolo 11 a disposizione delle autorità nazionali competenti per un periodo che termina dieci anni dopo che il sistema di IA per finalità generali è stato immesso sul mercato dell'Unione o messo in servizio nell'Unione.

5. I fornitori di sistemi di IA per finalità generali cooperano con altri fornitori che intendono mettere in servizio o immettere tali sistemi sul mercato dell'Unione come sistemi di IA ad alto rischio o come componenti di sistemi di IA ad alto rischio e forniscono loro le informazioni necessarie, nell'ottica di consentire a tali altri fornitori di rispettare i loro obblighi a norma del presente regolamento. Tale cooperazione tra fornitori preserva, se del caso, i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali in conformità dell'articolo 70. Al fine di garantire condizioni uniformi di esecuzione del presente regolamento per quanto riguarda le informazioni che i fornitori di sistemi di IA per finalità generali sono tenuti a condividere, la Commissione può adottare atti di esecuzione secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

6. Ai fini del rispetto dei requisiti e degli obblighi di cui ai paragrafi 1, 2 e 3:

- qualsiasi riferimento alla finalità prevista è inteso come riferimento all'eventuale uso dei sistemi di IA per finalità generali come sistemi di IA ad alto rischio o come componenti di sistemi di IA ad alto rischio ai sensi dell'articolo 6;

- qualsiasi riferimento ai requisiti per i sistemi di IA ad alto rischio di cui al titolo III, capo II, si intende fatto unicamente ai requisiti di cui al presente articolo.

Articolo 4 quater

Eccezioni all'articolo 4 ter

1. L'articolo 4 ter non si applica se il fornitore ha esplicitamente escluso tutti gli usi ad alto rischio nelle istruzioni per l'uso o nelle informazioni che accompagnano il sistema di IA per finalità generali.

2. Tale esclusione è effettuata in buona fede e non è ritenuta giustificata se il fornitore ha motivi sufficienti per ritenere che il sistema possa essere utilizzato impropriamente.

3. Qualora rilevi o sia informato di usi impropri del mercato, il fornitore adotta tutte le misure necessarie e proporzionate per prevenire ulteriori usi impropri, in particolare tenendo conto della portata dell'uso improprio e della gravità dei rischi associati.

TITOLO II

PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE

Articolo 5

1. Sono vietate le pratiche di intelligenza artificiale 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 con l'obiettivo o l'effetto di distorcerne materialmente il comportamento in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno fisico o psicologico;

   b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità 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 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 fisico o psicologico;

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

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

d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico da parte delle autorità di contrasto o per loro conto a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi:

i) la ricerca mirata di potenziali vittime specifiche di reato;

ii) la prevenzione di una minaccia specifica e sostanziale per l'infrastruttura critica, la vita, la salute o l'incolumità fisica delle persone fisiche o la prevenzione di attacchi terroristici;

iii) la localizzazione o l'identificazione di una persona fisica ai fini dello svolgimento di un'indagine penale, dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio[32], e punibili nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, o per altri reati specifici punibili nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno cinque anni, come stabilito dalla legge di tale Stato membro.

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, lettera d), tiene conto dei seguenti elementi:

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

[32] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

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, lettera d), rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali.

3. Per quanto riguarda il paragrafo 1, lettera d), e il 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 dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. 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 durante l'uso del sistema di IA e, qualora tale autorizzazione sia rifiutata, il suo utilizzo sia interrotto con effetto immediato.

L'autorità giudiziaria o amministrativa competente 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, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2.

4. 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, lettera d), e ai paragrafi 2 e 3. Tale Stato membro stabilisce 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, lettera d), compresi i reati di cui al punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto.

TITOLO III

SISTEMI DI IA AD ALTO RISCHIO

CAPO 1

CLASSIFICAZIONE DEI SISTEMI DI IA COME "AD ALTO RISCHIO"

Articolo 6

Regole di classificazione per i sistemi di IA ad alto rischio

1. Un sistema di IA che è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II è considerato ad alto rischio se 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 suddetta normativa.

2. Un sistema di IA destinato a essere utilizzato come componente di sicurezza di un prodotto disciplinato dalla normativa di cui al paragrafo 1 è considerato ad alto rischio se è tenuto a essere oggetto di 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 suddetta normativa. Tale disposizione si applica a prescindere dal fatto che il sistema di IA sia immesso sul mercato o messo in servizio in modo indipendente rispetto al prodotto.

3. I sistemi di IA di cui all'allegato III sono considerati ad alto rischio a meno che l'output del sistema non sia puramente accessorio in relazione alla pertinente azione o decisione da adottare e non sia pertanto suscettibile di comportare un rischio significativo per la salute, la sicurezza o i diritti fondamentali.

Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, la Commissione adotta, entro un anno dall'entrata in vigore del presente regolamento, atti di esecuzione per specificare le circostanze in cui gli output dei sistemi di IA di cui all'allegato III sarebbero puramente accessori rispetto alla pertinente azione o decisione da adottare. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 7

Modifiche dell'allegato III

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di modificare l'elenco di cui all'allegato III aggiungendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati ai punti da 1 a 8 dell'allegato III;

b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali, che è, in relazione alla sua gravità e alla probabilità che si verifichi, equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.

2. Nel valutare, ai fini del paragrafo 1, se un sistema di IA presenti un rischio di danno per la salute e la sicurezza o un rischio di impatto negativo sui diritti fondamentali equivalente o superiore al rischio di danno presentato dai sistemi di IA ad alto rischio di cui all'allegato III, la Commissione tiene conto dei criteri seguenti:

a) la finalità prevista del sistema di IA;

b) la misura in cui un sistema di IA è stato usato o è probabile che sarà usato;

c) la misura in cui l'uso di un sistema di IA ha già causato un danno alla salute e alla sicurezza o un impatto negativo sui diritti fondamentali o ha suscitato gravi preoccupazioni in relazione al verificarsi di tale danno o impatto negativo, come dimostrato da relazioni o da prove documentate presentate alle autorità nazionali competenti;

d) la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e capacità di incidere su una pluralità di persone;

e) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo dipendono dal risultato prodotto da un sistema di IA, in particolare perché per motivi pratici o giuridici non è ragionevolmente possibile sottrarsi a tale risultato;

f) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto all'utente di un sistema di IA, in particolare a causa di uno squilibrio di potere, conoscenza, situazione economica o sociale o età;

g) la misura in cui il risultato prodotto con un sistema di IA non è facilmente reversibile, considerando non facilmente reversibili i risultati che hanno un impatto sulla salute o sulla sicurezza delle persone;

h) la misura in cui la legislazione vigente dell'Unione prevede:

i) misure di ricorso efficaci in relazione ai rischi presentati da un sistema di IA, ad esclusione delle richieste di risarcimento del danno;

ii) misure efficaci per prevenire o ridurre sostanzialmente tali rischi;

i) l'entità e la probabilità dei benefici derivanti dall'utilizzo dell'IA per i singoli, i gruppi o la società in generale.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di modificare l'elenco di cui all'allegato III rimuovendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) il sistema o i sistemi di IA ad alto rischio interessati non pongono più rischi significativi per i diritti fondamentali, la salute o la sicurezza, tenendo conto dei criteri elencati al paragrafo 2;

b) la soppressione non riduce il livello generale di protezione della salute, della sicurezza e dei diritti fondamentali a norma del diritto dell'Unione.

CAPO 2

REQUISITI PER I SISTEMI DI IA AD ALTO RISCHIO

Articolo 8

Conformità ai requisiti

1. I sistemi di IA ad alto rischio rispettano i requisiti stabiliti nel presente capo, tenendo conto dello stato dell'arte generalmente riconosciuto.

2. Nel garantire conformità a tali requisiti si tiene conto della finalità prevista del sistema di IA ad alto rischio e del sistema di gestione dei rischi di cui all'articolo 9.

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 aggiornamento costante e sistematico. Esso comprende le fasi seguenti:

   a) identificazione e analisi dei rischi noti e prevedibili più probabili per la salute, la sicurezza e i diritti fondamentali in considerazione della finalità prevista del sistema di IA ad alto rischio;

   b) [soppresso];

   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 61;

   d) adozione di adeguate misure di gestione dei rischi conformemente alle disposizioni dei paragrafi seguenti.

   I rischi di cui al presente paragrafo 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.

3. 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 al presente capo 2, 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.

4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che qualsiasi rischio residuo associato 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 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 in relazione ai rischi che non possono essere eliminati;

c) la fornitura di informazioni adeguate a norma dell'articolo 13, in particolare per quanto riguarda i rischi di cui al paragrafo 2, lettera b), e, ove opportuno, la formazione degli utenti.

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 dall'utente e l'ambiente in cui il sistema è destinato ad essere usato.

5. I sistemi di IA ad alto rischio sono sottoposti a prova per garantire che essi funzionino in modo coerente con la finalità prevista e che siano conformi ai requisiti di cui al presente capo.

6. Le procedure di prova possono comprendere prove in condizioni reali conformemente all'articolo 54 bis.

7. 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 dell'immissione sul mercato o della messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite in via preliminare e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio.

8. Il sistema di gestione dei rischi di cui ai paragrafi da 1 a 7 presta particolare attenzione all'eventualità che il sistema di IA ad alto rischio sia accessibile alle persone di età inferiore a 18 anni o abbia un impatto su di esse.

9. Per i fornitori di sistemi di IA ad alto rischio soggetti ai requisiti relativi ai processi interni di gestione dei rischi a norma del pertinente diritto settoriale dell'Unione, gli aspetti descritti ai paragrafi da 1 a 8 possono far parte delle procedure di gestione dei rischi stabilite a norma di tale diritto.

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 sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5.

2. I set di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di governance e gestione dei dati. Tali pratiche riguardano in particolare:

   a) le scelte progettuali pertinenti;

   b) i processi di raccolta dei dati;

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

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

e) una valutazione preliminare 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 fisiche o comportare discriminazioni vietate dal diritto dell'Unione;

g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi e, nella misura del possibile, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui 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 di una combinazione degli stessi.

4. I set di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, 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 monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari 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, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

6. Per lo sviluppo di sistemi di IA ad alto rischio che non utilizzano tecniche che prevedono l'addestramento di modelli, i paragrafi da 2 a 5 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.

   La documentazione tecnica è redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui al presente capo e fornisce alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, tutte le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV o, nel caso delle PMI, incluse le start-up, qualsiasi documentazione equivalente che soddisfi i medesimi obiettivi, a meno che ciò non sia ritenuto inappropriato dall'autorità competente.

2. Se è immesso sul mercato o messo in servizio un sistema di IA ad alto rischio connesso a un prodotto al quale si applicano gli atti giuridici elencati nell'allegato II, sezione A, si redige un'unica documentazione tecnica contenente tutte le informazioni di cui all'allegato IV e le informazioni necessarie a norma di tali atti giuridici.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 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 al presente capo.

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 adeguato alla finalità prevista del sistema, le capacità di registrazione consentono la registrazione di eventi pertinenti per:

   i) l'individuazione di situazioni che possono far sì che il sistema di IA presenti un rischio ai sensi dell'articolo 65, paragrafo 1, o determinare una modifica sostanziale;

   ii) l'agevolazione del monitoraggio successivo all'immissione sul mercato di cui all'articolo 61; nonché

   iii)il monitoraggio del funzionamento dei sistemi di IA ad alto rischio di cui all'articolo 29, paragrafo 4.

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

   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 con cui il sistema ha verificato 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 13

Trasparenza e fornitura di informazioni agli utenti

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente al fine di conseguire il rispetto dei pertinenti obblighi dell'utente e del fornitore di cui al capo 3 del presente titolo e consentire agli utenti di comprendere e utilizzare adeguatamente il sistema.

2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso in un formato digitale o non digitale appropriato, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per gli utenti.

3. Le informazioni di cui al paragrafo 2 specificano:

   a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato;

   b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:

      i) la sua finalità prevista, compreso lo specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere utilizzato;

      ii) il livello di accuratezza, comprese le metriche, di robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza;

      iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'articolo 9, paragrafo 2;

iv) ove opportuno, il suo comportamento per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato;

v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA;

vi) ove opportuno, una descrizione dell'output atteso del sistema;

c) le eventuali 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;

d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti;

e) le risorse computazionali e di hardware necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza, necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software;

f) una descrizione del meccanismo incluso nel sistema di IA che consente agli utenti di raccogliere, conservare e interpretare correttamente i log, se del caso.

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 il sistema di IA è 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 quando tali rischi persistono nonostante l'applicazione di altri requisiti di cui al presente capo.

3. La sorveglianza umana è garantita mediante almeno uno dei seguenti tipi di misure:

   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 dall'utente.

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

   a) comprendere le capacità e i limiti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento;

   b) restare consapevoli 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");

   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 di interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga.

5. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 sono tali da garantire che, inoltre, l'utente non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che essa non sia stata verificata e confermata separatamente da almeno due persone fisiche. 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, nei casi in cui il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito.

Articolo 15

Accuratezza, robustezza e cibersicurezza

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.

2. I livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di IA ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.

3. I sistemi di IA ad alto rischio sono resilienti per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi.

   La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe.

   I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano gli input per operazioni future ("circuiti di feedback", feedback loops) e garantire che tali output potenzialmente distorti siano oggetto di adeguate misure di attenuazione.

4. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso o le prestazioni sfruttando le vulnerabilità del sistema.

Le soluzioni tecniche volte a garantire la cibersicurezza dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti.

Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire e controllare gli attacchi che cercano di manipolare il set di dati di addestramento ("avvelenamento dei dati", data poisoning), gli input progettati in modo da far sì che il modello commetta un errore ("esempi antagonistici", adversarial examples) o i difetti del modello.

CAPO 3

OBBLIGHI DEI FORNITORI E DEGLI UTENTI DEI SISTEMI DI IA AD ALTO RISCHIO E DI ALTRE PARTI

Articolo 16

Obblighi dei fornitori dei sistemi di IA ad alto rischio

I fornitori dei sistemi di IA ad alto rischio:

(a) garantiscono che i loro sistemi di IA ad alto rischio siano conformi ai requisiti di cui al capo 2 del presente titolo;

a bis) indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato, l'indirizzo al quale possono essere contattati sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o in un documento di accompagnamento;

b) dispongono di un sistema di gestione della qualità conforme all'articolo 17;

c) conservano la documentazione ai sensi dell'articolo 18;

d) quando sono sotto il loro controllo, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio di cui all'articolo 20;

e) garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima della sua immissione sul mercato o messa in servizio;

f) rispettano gli obblighi di registrazione di cui all'articolo 51, paragrafo 1;

g) adottano le necessarie misure correttive di cui all'articolo 21, se il sistema di IA ad alto rischio non è conforme ai requisiti di cui al capo 2 del presente titolo;

h) informano la pertinente autorità nazionale competente degli Stati membri in cui hanno messo a disposizione o messo in servizio il sistema di IA e, ove applicabile, l'organismo notificato in merito alla non conformità e alle eventuali misure correttive adottate;

i) appongono la marcatura CE sui loro sistemi di IA ad alto rischio per indicare la conformità al presente regolamento a norma dell'articolo 49;

j) su richiesta di un'autorità nazionale competente, dimostrano la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo.

Articolo 17

Sistema di gestione della qualità

1. I fornitori di sistemi di IA ad alto rischio istituiscono di 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 i seguenti aspetti:

   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, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme ai requisiti di cui al capo 2 del presente titolo;

f) i sistemi e le procedure per la gestione dei dati, compresa 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 61;

i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 62;

j) la gestione della comunicazione con le autorità nazionali competenti, le autorità competenti, comprese quelle settoriali, 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.

2 bis. Per i fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità a norma del pertinente diritto settoriale dell'Unione, gli aspetti descritti al paragrafo 1 possono far parte dei sistemi di gestione della qualità stabiliti a norma di tale diritto.

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

Articolo 18

Conservazione dei documenti

1. Il fornitore, per un periodo che termina 10 anni dopo che il sistema di IA è stato immesso sul mercato o messo in servizio, tiene a disposizione delle autorità nazionali competenti:

a) la documentazione tecnica di cui all'articolo 11;

b) la documentazione relativa al sistema di gestione della qualità di cui all'articolo 17;

c) la documentazione relativa alle modifiche approvate dagli organismi notificati, ove applicabile;

d) le decisioni e gli altri documenti rilasciati dagli organismi notificati, ove applicabile;

e) la dichiarazione di conformità UE di cui all'articolo 48.

1 bis. Ciascuno Stato membro stabilisce le condizioni alle quali la documentazione di cui al paragrafo 1 resta a disposizione delle autorità nazionali competenti per il periodo indicato in tale paragrafo in caso di fallimento o cessazione delle attività, prima della fine di tale periodo, del prestatore o del rappresentante autorizzato stabilito nel suo territorio.

2. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della legislazione dell'Unione sui servizi finanziari conservano la documentazione tecnica come parte della documentazione conservata a norma della pertinente legislazione dell'Unione in materia di servizi finanziari.

Articolo 19

Valutazione della conformità

1. I fornitori dei sistemi di IA ad alto rischio garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima della sua immissione sul mercato o messa in servizio. Se in seguito a tale valutazione i sistemi di IA risultano conformi ai requisiti di cui al capo 2 del presente titolo, i fornitori redigono una dichiarazione di conformità UE a norma dell'articolo 48 e appongono la marcatura CE di conformità a norma dell'articolo 49.

2. [soppresso]

Articolo 20

Log generati automaticamente

1. I fornitori di sistemi di IA ad alto rischio conservano i log, di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo in virtù di un accordo contrattuale con l'utente o in forza di legge. Essi li conservano per un periodo di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, segnatamente il diritto dell'Unione in materia di protezione dei dati personali.

2. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della legislazione dell'Unione sui servizi finanziari mantengono i log generati automaticamente dai loro sistemi di IA ad alto rischio nell'ambito della documentazione conservata a norma della pertinente legislazione in materia di servizi finanziari.

Articolo 21

Misure correttive

I fornitori di sistemi di IA ad alto rischio che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non sia conforme al presente regolamento procedono immediatamente, se del caso, a un'indagine delle cause in collaborazione con l'utente che ha effettuato la segnalazione e adottano le misure correttive necessarie per rendere conforme tale dispositivo, ritirarlo o richiamarlo, a seconda dei casi. Essi informano di conseguenza i distributori del sistema di IA ad alto rischio in questione e, ove applicabile, il rappresentante autorizzato e gli importatori.

Articolo 22

Dovere di informazione

Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, e tale rischio sia noto al fornitore del sistema, tale fornitore informa immediatamente le autorità nazionali competenti degli Stati membri in cui ha messo a disposizione il sistema e, ove applicabile, l'organismo notificato che ha rilasciato un certificato per il sistema di IA ad alto rischio, in particolare in merito alla non conformità e alle eventuali misure correttive adottate.

Articolo 23

Cooperazione con le autorità competenti

I fornitori di sistemi di IA ad alto rischio, su richiesta di un'autorità nazionale competente, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, in una lingua che può essere compresa facilmente dall'autorità dello Stato membro interessato. Su richiesta motivata di un'autorità nazionale competente, i fornitori forniscono a tale autorità l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo in virtù di un accordo contrattuale con l'utente o in forza di legge.

Articolo 23 bis

Condizioni per l'assoggettamento di terzi agli obblighi di un fornitore

1. Qualsiasi persona fisica o giuridica è considerata un fornitore di un nuovo sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetta 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;

b) [soppresso]

c) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio;

d) se modifica la finalità prevista di un sistema di IA che non è considerato ad alto rischio ed è già immesso sul mercato o messo in servizio in maniera tale da far sì che il sistema modificato diventi un sistema di IA ad alto rischio;

e) se immette sul mercato o mette in servizio un sistema di IA per finalità generali come sistema di IA ad alto rischio o come componente di un sistema di IA ad alto rischio.

2. Qualora si verifichino le circostanze di cui al paragrafo 1, lettera a) o c), il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA ad alto rischio non è più considerato un fornitore ai fini del presente regolamento.

3. Per i sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti cui si applicano gli atti giuridici elencati nell'allegato II, sezione A, il fabbricante di tali prodotti 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:

i) 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;

ii) 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.

Articolo 24

[soppresso]

Articolo 25

Rappresentanti autorizzati

1. Prima di mettere a disposizione i propri sistemi sul mercato dell'Unione, i fornitori stabiliti al di fuori dell'Unione nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fabbricante. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire solo i seguenti compiti:

-a) verificare che la dichiarazione di conformità UE e la documentazione tecnica siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità;

a) tenere a disposizione delle autorità nazionali competenti e delle autorità nazionali di cui all'articolo 63, paragrafo 7, per un periodo di 10 anni dopo la data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, i dati di contatto del fornitore che ha nominato il rappresentante autorizzato, una copia della dichiarazione di conformità UE, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato;

b) fornire all'autorità nazionale competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle conservate conformemente alla lettera b), necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, compreso l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore in virtù di un accordo contrattuale con l'utente o in forza di legge;

c) cooperare con le autorità nazionali competenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio.

d) rispettare gli obblighi di registrazione di cui all'articolo 51, paragrafo 1, e, se la registrazione del sistema è effettuata dal fornitore stesso, verificare la correttezza delle informazioni di cui all'allegato VIII, parte II, punti da 1 a 11.

Il rappresentante autorizzato pone fine al mandato se ha motivi sufficienti per ritenere che il fornitore agisca in contrasto con i propri obblighi ai sensi del presente regolamento. In tal caso, comunica immediatamente all'autorità di vigilanza del mercato dello Stato membro in cui è stabilito — nonché, se del caso, all'organismo notificato pertinente — la cessazione del mandato e i relativi motivi.

Il rappresentante autorizzato è giuridicamente responsabile per i sistemi di IA difettosi sulla stessa base del fornitore e in solido con esso per quanto riguarda la sua potenziale responsabilità a norma della direttiva 85/374/CEE del Consiglio.

Articolo 26

Obblighi degli importatori

1. Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori di tale sistema garantiscono che sia conforme al presente regolamento verificando che:

a) il fornitore di tale sistema di IA abbia eseguito la pertinente procedura di valutazione della conformità di cui all'articolo 43;

b) il fornitore abbia redatto la documentazione tecnica conformemente all'allegato IV;

c) il sistema rechi la necessaria marcatura di conformità CE e sia accompagnato dalla dichiarazione di conformità UE e dalle istruzioni per l'uso;

d) il fornitore abbia designato il rappresentante autorizzato di cui all'articolo 25.

2. Qualora abbia motivi sufficienti di ritenere che un sistema di IA ad alto rischio non sia conforme al presente regolamento, ovvero sia falsificato o sia accompagnato da una documentazione falsificata, un importatore non lo immette sul mercato fino a quando tale sistema di IA non sia stato reso conforme. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, l'importatore ne informa il fornitore del sistema di IA, i rappresentanti autorizzati e le autorità di vigilanza del mercato.

3. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o in un documento di accompagnamento.

4. Gli importatori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità ai requisiti di cui al capo 2 del presente titolo.

4 bis. Gli importatori conservano, per un periodo di 10 anni dalla data di immissione sul mercato o di messa in servizio del sistema di IA, una copia del certificato rilasciato dall'organismo notificato, se del caso, delle istruzioni per l'uso e della dichiarazione di conformità UE.

5. Gli importatori forniscono all'autorità nazionale competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle conservate conformemente al paragrafo 5, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo in una lingua che può essere compresa facilmente da tale autorità nazionale competente. A tal fine garantiscono altresì che la documentazione tecnica possa essere messa a disposizione di tale autorità.

5 bis. Gli importatori cooperano con le autorità nazionali competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione a un sistema di IA di cui sono importatori.

Articolo 27

Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che il sistema di IA ad alto rischio rechi la necessaria marcatura CE di conformità, che sia accompagnato da una copia della dichiarazione di conformità UE e dalle istruzioni per l'uso e che il fornitore e l'importatore del sistema, a seconda dei casi, abbiano rispettato i loro obblighi di cui, rispettivamente, all'articolo 16, lettera b), e all'articolo 26, paragrafo 3.

2. Qualora ritenga o abbia motivo di ritenere che un sistema di IA ad alto rischio non sia conforme ai requisiti di cui al capo 2 del presente titolo, un distributore non lo mette a disposizione sul mercato fino a quando tale sistema di IA ad alto rischio non sia stato reso conforme a tali requisiti. Inoltre, qualora il sistema presenti un rischio ai sensi dell'articolo 65, paragrafo 1, il distributore ne informa il fornitore o l'importatore del sistema, a seconda dei casi.

3. I distributori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità del sistema ai requisiti di cui al capo 2 del presente titolo.

4. Un distributore che ritiene o ha motivo di ritenere che un sistema di IA ad alto rischio che ha messo a disposizione sul mercato non sia conforme ai requisiti di cui al capo 2 del presente titolo adotta le misure correttive necessarie per rendere tale sistema conforme a tali requisiti, ritirarlo o richiamarlo o garantisce che il fornitore, l'importatore o qualsiasi operatore pertinente, a seconda dei casi, adotti tali misure correttive. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 65, paragrafo 1, il distributore ne informa immediatamente le autorità nazionali competenti degli Stati membri in cui ha messo il prodotto a disposizione, fornendo in particolare informazioni precise sulla non conformità e sulle eventuali misure correttive adottate.

5. Su richiesta motivata di un'autorità nazionale competente, i distributori di sistemi di IA ad alto rischio forniscono a tale autorità tutte le informazioni e la documentazione concernenti le attività descritte ai paragrafi da 1 a 4.

5 bis. I distributori cooperano con le autorità nazionali competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione a un sistema di IA di cui sono distributori.

Articolo 28

[soppresso]

Articolo 29

Obblighi degli utenti dei sistemi di IA ad alto rischio

1. Gli utenti di sistemi di IA ad alto rischio usano tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 2 e 5.

1 bis. Gli utenti affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie.

2. Gli obblighi di cui ai paragrafi 1 e 1 bis lasciano impregiudicati gli altri obblighi degli utenti previsti dal diritto dell'Unione o nazionale e la discrezionalità dell'utente nell'organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.

3. Fatto salvo il paragrafo 1, nella misura in cui esercita il controllo sui dati di input, l'utente garantisce che tali dati di input siano pertinenti alla luce della finalità prevista del sistema di IA ad alto rischio.

4. Gli utenti attuano la sorveglianza umana e monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso. Se hanno motivo di ritenere che l'uso in conformità alle istruzioni per l'uso possa far sì che il sistema di IA presenti un rischio ai sensi dell'articolo 65, paragrafo 1, ne informano il fornitore o il distributore e sospendono l'uso del sistema. Essi informano inoltre il fornitore o il distributore qualora abbiano individuato un incidente grave e interrompono l'uso del sistema di IA. Nel caso in cui l'utente non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 62. Tale obbligo non riguarda i dati operativi sensibili degli utenti dei sistemi di IA che sono autorità di contrasto.

Per gli utenti che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della legislazione dell'Unione sui servizi finanziari, l'obbligo di monitoraggio di cui al primo comma si considera soddisfatto se sono soddisfatte le regole sui dispositivi, i processi e i meccanismi di governance interna di cui alla pertinente legislazione in materia di servizi finanziari.

5. Gli utenti di sistemi di IA ad alto rischio conservano i log, di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo. Essi li conservano per un periodo di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, segnatamente il diritto dell'Unione in materia di protezione dei dati personali.

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

5 bis. Gli utenti di sistemi di IA ad alto rischio che sono autorità, agenzie o organismi pubblici, ad eccezione delle autorità di contrasto e delle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo, rispettano gli obblighi di registrazione di cui all'articolo 51. Ove accertino che il sistema che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 60, non utilizzano tale sistema e ne informano il fornitore o il distributore.

6. Gli utenti di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 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, ove applicabile.

6 bis. Gli utenti cooperano con le autorità nazionali competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione a un sistema di IA di cui sono utenti.

CAPO 4

AUTORITÀ DI NOTIFICA E ORGANISMI NOTIFICATI

Articolo 30

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.

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 attività eseguite dagli organismi di valutazione della conformità o servizi di consulenza su base commerciale o concorrenziale.

6. Le autorità di notifica salvaguardano la riservatezza delle informazioni ottenute conformemente all'articolo 70.

7. Le autorità di notifica dispongono di un numero adeguato di dipendenti competenti per l'adeguata esecuzione dei relativi compiti.

8. [soppresso]

Articolo 31

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 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 33. 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 33. 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 a sostegno della loro procedura di designazione a norma del presente regolamento, a seconda dei casi. L'organismo notificato aggiorna la documentazione di cui ai paragrafi 2 e 3 ogniqualvolta si verifichino 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 33.

Articolo 32

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 33.

2. Le autorità di notifica notificano tali organismi alla Commissione e agli altri Stati membri utilizzando lo strumento elettronico di notifica elaborato e gestito dalla Commissione.

3. La notifica di cui al paragrafo 2 include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità e i 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 31, 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 disposizioni predisposte per fare in modo che tale organismo sia monitorato periodicamente e continui a soddisfare le prescrizioni di cui all'articolo 33.

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 da una notifica da parte di un'autorità di notifica, qualora essa includa un certificato di accreditamento di cui all'articolo 31, paragrafo 2, o entro due mesi da una notifica da parte dell'autorità di notifica qualora essa includa le prove documentali di cui all'articolo 31, paragrafo 3.

5. [soppresso]

Articolo 33

Prescrizioni relative agli organismi notificati

1. Un organismo notificato è istituito a norma del diritto nazionale e ha personalità giuridica.

2. Gli organismi notificati soddisfano i requisiti organizzativi, di gestione della qualità e relativi alle risorse e ai processi necessari all'assolvimento dei loro compiti.

3. La struttura organizzativa, l'assegnazione delle responsabilità, le linee di riporto e il funzionamento degli organismi notificati sono tali da garantire la fiducia nelle prestazioni degli organismi notificati e nei risultati delle attività di valutazione della conformità che essi effettuano.

4. Gli organismi notificati sono indipendenti dal fornitore di un sistema di IA ad alto rischio in relazione al quale svolgono attività di valutazione della conformità. Gli organismi notificati sono inoltre indipendenti da qualsiasi altro operatore avente un interesse economico nel sistema di IA ad alto rischio oggetto della valutazione, nonché da eventuali concorrenti del fornitore.

5. Gli organismi notificati sono organizzati e gestiti in modo da salvaguardare l'indipendenza, l'obiettività e l'imparzialità delle loro attività. Gli organismi notificati documentano e attuano una struttura e procedure per salvaguardare l'imparzialità e per promuovere e applicare i principi di imparzialità in tutta l'organizzazione, tra il personale e nelle attività di valutazione.

6. Gli organismi notificati dispongono di procedure documentate per garantire che il loro personale, i loro comitati, affiliate, subappaltatori e qualsiasi altra organizzazione associata o il personale di organismi esterni rispettino la riservatezza delle informazioni, conformemente all'articolo 70, di cui vengono in possesso nello svolgimento delle attività di valutazione della conformità, salvo quando la legge ne prescriva la divulgazione. Il personale degli organismi notificati è tenuto a osservare il segreto professionale riguardo a tutte le informazioni ottenute nello svolgimento dei suoi compiti a norma del presente regolamento, tranne che nei confronti delle autorità di notifica dello Stato membro in cui svolge le sue attività.

7. Gli organismi notificati dispongono di procedure per svolgere le attività che tengono debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA in questione.

8. Gli organismi notificati sottoscrivono un'adeguata assicurazione di responsabilità per le loro attività di valutazione della conformità, a meno che lo Stato membro in cui sono ubicati non si assuma tale responsabilità a norma del diritto interno o non sia esso stesso direttamente responsabile della valutazione della conformità.

9. Gli organismi notificati sono in grado di eseguire tutti i compiti assegnati loro in forza del presente regolamento con il più elevato grado di integrità professionale e di competenza richiesta nel settore specifico, indipendentemente dal fatto che tali compiti siano eseguiti dagli organismi notificati stessi o per loro conto e sotto la loro responsabilità.

10. Gli organismi notificati dispongono di sufficienti competenze interne per poter valutare efficacemente i compiti svolti da parti esterne per loro conto. Gli organismi notificati dispongono permanentemente di sufficiente personale amministrativo, tecnico, giuridico e scientifico dotato di esperienza e conoscenze relative alle tecnologie, ai dati e al calcolo dei dati di intelligenza artificiale pertinenti, nonché ai requisiti di cui al capo 2 del presente titolo.

11. Gli organismi notificati partecipano alle attività di coordinamento di cui all'articolo 38. Inoltre essi partecipano direttamente o sono rappresentati in seno alle organizzazioni europee di normazione o garantiscono di essere informati e di mantenersi aggiornati in merito alle norme pertinenti.

12. [soppresso]

Articolo 33 bis

Presunzione di conformità alle prescrizioni relative agli organismi notificati

Qualora dimostri la propria conformità ai criteri stabiliti nelle pertinenti norme armonizzate o in parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, l'organismo di valutazione della conformità è considerato conforme alle prescrizioni di cui all'articolo 33 nella misura in cui le norme armonizzate applicabili coprano tali prescrizioni.

Articolo 34

Affiliate e subappaltatori degli organismi notificati

1. L'organismo notificato, qualora subappalti compiti specifici connessi alla valutazione della conformità oppure ricorra a un'affiliata, garantisce che il subappaltatore o l'affiliata soddisfino i requisiti di cui all'articolo 33 e ne informa l'autorità di notifica.

2. Gli organismi notificati si assumono la completa responsabilità dei compiti eseguiti da subappaltatori o affiliate, ovunque questi siano stabiliti.

3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fornitore.

4. I documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento sono tenuti a disposizione dell'autorità di notifica per un periodo di cinque anni a decorrere dalla data di cessazione dell'attività di subappalto.

Articolo 34 bis

Obblighi operativi degli organismi notificati

1. Gli organismi notificati verificano la conformità del sistema di IA ad alto rischio secondo le procedure di valutazione della conformità di cui all'articolo 43.

2. Gli organismi notificati svolgono le proprie attività evitando oneri inutili per i fornitori e tenendo debitamente conto delle dimensioni di un'impresa, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA ad alto rischio in questione. Nel far ciò l'organismo notificato rispetta tuttavia il grado di rigore e il livello di tutela necessari per la conformità del sistema di IA ad alto rischio rispetto ai requisiti del presente regolamento.

3. Gli organismi notificati mettono a disposizione e trasmettono su richiesta tutta la documentazione pertinente, inclusa la documentazione del fornitore, all'autorità di notifica di cui all'articolo 30 per consentirle di svolgere le proprie attività di valutazione, designazione, notifica e monitoraggio e per agevolare la valutazione di cui al presente capo.

Articolo 35

Numeri di identificazione e liste di organismi notificati designati a norma del presente regolamento

1. La Commissione assegna un numero di identificazione agli organismi notificati. Essa assegna un numero unico anche se un organismo è notificato a norma di diversi atti dell'Unione.

2. La Commissione mette pubblicamente a disposizione l'elenco degli organismi notificati a norma del presente regolamento, inclusi i numeri di identificazione loro assegnati e le attività per le quali sono stati notificati. La Commissione garantisce che l'elenco sia tenuto aggiornato.

Articolo 36

Modifiche delle notifiche

1. L'autorità di notifica informa la Commissione e gli altri Stati membri di eventuali modifiche pertinenti della notifica di un organismo notificato tramite lo strumento elettronico di notifica di cui all'articolo 32, paragrafo 2.

2. Le procedure di cui agli articoli 31 e 32 si applicano alle estensioni della portata della notifica. In caso di modifiche della notifica diverse da estensioni della sua portata, si applicano le procedure stabilite nei paragrafi che seguono.

Qualora decida di cessare le attività di valutazione della conformità, un organismo notificato ne informa l'autorità di notifica e i fornitori interessati quanto prima possibile e un anno prima della cessazione delle attività qualora la cessazione sia stata programmata. Il certificato può restare valido per un periodo temporaneo di nove mesi dopo la cessazione delle attività dell'organismo notificato purché un altro organismo notificato abbia confermato per iscritto che assumerà la responsabilità per i sistemi di IA coperti da tale certificato. Il nuovo organismo notificato completa una valutazione integrale dei sistemi di IA coinvolti entro la fine del periodo indicato prima di rilasciare nuovi certificati per gli stessi sistemi. Qualora l'organismo notificato abbia cessato le proprie attività, l'autorità di notifica ritira la designazione.

3. Qualora un'autorità di notifica abbia motivi sufficienti per ritenere che un organismo notificato non soddisfa più i requisiti di cui all'articolo 33 o non adempie i suoi obblighi, l'autorità di notifica, a condizione che l'organismo notificato abbia avuto la possibilità di esprimere il suo punto di vista, limita, sospende o ritira la notifica, a seconda dei casi, in funzione della gravità del mancato rispetto di tali requisiti o dell'inadempimento di tali obblighi. Essa ne informa immediatamente la Commissione e gli altri Stati membri.

4. Qualora la sua designazione sia stata sospesa, limitata oppure ritirata interamente o in parte, l'organismo notificato informa i fabbricanti interessati al più tardi entro 10 giorni.

5. In caso di limitazione, sospensione o ritiro di una notifica, l'autorità di notifica adotta le misure appropriate per far sì che i fascicoli dell'organismo notificato in questione siano conservati e messi a disposizione delle autorità di notifica in altri Stati membri nonché delle autorità di vigilanza del mercato, su richiesta.

6. In caso di limitazione, sospensione o ritiro di una designazione, l'autorità di notifica:

   a) valuta l'impatto sui certificati rilasciati dall'organismo notificato;

   b) entro tre mesi dalla comunicazione delle modifiche della notifica, presenta alla Commissione e agli altri Stati membri una relazione sulle proprie constatazioni;

   c) impone all'organismo notificato di sospendere o ritirare, entro un periodo di tempo ragionevole stabilito dall'autorità, i certificati rilasciati indebitamente al fine di garantire la conformità dei sistemi di IA sul mercato;

   d) informa la Commissione e gli Stati membri in merito ai certificati di cui ha richiesto la sospensione o il ritiro;

e) fornisce alle autorità nazionali competenti dello Stato membro in cui ha sede il fornitore tutte le informazioni pertinenti sui certificati di cui ha richiesto la sospensione o il ritiro. Tale autorità competente adotta le misure appropriate, laddove necessario, per evitare un rischio potenziale per la salute, la sicurezza o i diritti fondamentali.

7. Ad eccezione dei certificati rilasciati indebitamente, e ove la notifica sia stata sospesa o limitata, i certificati restano validi nei seguenti casi:

a) l'autorità di notifica ha confermato, entro un mese dalla sospensione o dalla limitazione, che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i certificati oggetto di sospensione o limitazione e l'autorità di notifica ha predisposto un calendario e previsto azioni al fine di porre rimedio alla sospensione o alla limitazione; oppure

b) l'autorità di notifica ha confermato che durante il periodo di sospensione o di limitazione non saranno rilasciati, modificati o rinnovati certificati attinenti alla sospensione e indica se l'organismo notificato è in grado di continuare a svolgere il monitoraggio e rimanere responsabile dei certificati esistenti rilasciati durante il periodo della sospensione o della limitazione. Nel caso in cui l'autorità responsabile degli organismi notificati stabilisca che l'organismo notificato non è in grado di sostenere i certificati in vigore, il fornitore conferma per iscritto alle autorità nazionali competenti dello Stato membro in cui ha la propria sede il fornitore del sistema coperto dal certificato, entro tre mesi dalla sospensione o dalla limitazione, che un altro organismo notificato qualificato assume temporaneamente le funzioni dell'organismo notificato di svolgere il monitoraggio e assumere la responsabilità dei certificati durante il periodo di sospensione o limitazione.

8. Ad eccezione dei certificati rilasciati indebitamente, e ove la designazione sia stata ritirata, i certificati restano validi per un periodo di nove mesi nei seguenti casi:

a) l'autorità nazionale competente dello Stato membro in cui ha la propria sede il fornitore del sistema di IA coperto dal certificato ha confermato che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i sistemi in questione; e

b) un altro organismo notificato ha confermato per iscritto che assume immediatamente la responsabilità per i sistemi in questione e che completerà la valutazione degli stessi entro dodici mesi dal ritiro della designazione.

Nei casi di cui al primo comma, l'autorità nazionale competente dello Stato membro in cui ha la propria sede il fornitore del sistema coperto dal certificato può prorogare la validità temporanea dei certificati di ulteriori periodi di tre mesi, per un totale non superiore a dodici mesi.

L'autorità nazionale competente o l'organismo notificato che assume le funzioni dell'organismo notificato interessato dalla modifica della notifica informa immediatamente la Commissione, gli altri Stati membri e gli altri organismi notificati.

Articolo 37

Contestazione della competenza degli organismi notificati

1. Ove necessario, la Commissione indaga su tutti i casi in cui vi siano motivi di dubitare della conformità di un organismo notificato ai requisiti di cui all'articolo 33.

2. L'autorità di notifica fornisce alla Commissione, su richiesta, tutte le informazioni relative alla notifica dell'organismo notificato interessato.

3. La Commissione provvede affinché tutte le informazioni riservate ottenute nel corso delle sue indagini a norma del presente articolo siano trattate in maniera riservata in conformità dell'articolo 70.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa o non soddisfa più i requisiti di cui all'articolo 33, informa l'autorità di notifica dei motivi di tale accertamento e le chiede di adottare le misure correttive necessarie, compresi la sospensione, la limitazione o il ritiro della designazione, se del caso. Se l'autorità di notifica non adotta le misure correttive necessarie, la Commissione può, mediante atti di esecuzione, sospendere, limitare o ritirare la notifica. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Articolo 38

Coordinamento degli organismi notificati

1. La Commissione garantisce che, per quanto riguarda i sistemi di IA ad alto rischio, siano istituiti e funzionino correttamente, sotto forma di un gruppo settoriale di organismi notificati, un coordinamento e una cooperazione adeguati tra gli organismi notificati che partecipano alle procedure di valutazione della conformità a norma del presente regolamento.

2. L'autorità di notifica garantisce che gli organismi da essi notificati partecipino al lavoro di tale gruppo, direttamente o mediante rappresentanti designati.

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 di cui all'articolo 33.

CAPO 5

NORME, VALUTAZIONE DELLA CONFORMITÀ, CERTIFICATI, REGISTRAZIONE

Articolo 40

Norme armonizzate

1. I sistemi di IA ad alto rischio o i sistemi 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* si presumono conformi ai requisiti di cui al capo 2 del presente titolo o, se del caso, ai requisiti di cui agli articoli 4 bis e 4 ter, nella misura in cui tali requisiti sono contemplati da tali norme.

2. Nel presentare una richiesta di normazione alle organizzazioni europee di normazione conformemente all'articolo 10 del regolamento (UE) n. 1025/2012, la Commissione specifica che le norme sono coerenti, chiare e redatte in modo tale che mirino a conseguire, in particolare, i seguenti obiettivi:

   a) garantire che i sistemi di IA immessi sul mercato o messi in servizio nell'Unione siano sicuri e rispettino i valori dell'Unione e rafforzino l'autonomia strategica aperta dell'Unione;

   b) 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;

   c) rafforzare la governance multipartecipativa, con la rappresentanza di tutti i portatori di interessi europei (ad esempio l'industria, le PMI, la società civile, i ricercatori);

   d) contribuire a rafforzare la cooperazione globale in materia di normazione nel settore dell'IA in modo coerente con i valori e gli interessi dell'Unione.

   La Commissione chiede alle organizzazioni europee di normazione di dimostrare che si adoperano al massimo per conseguire gli obiettivi di cui sopra.

Articolo 41

Specifiche comuni

1. Alla Commissione è conferito il potere di adottare, previa consultazione del comitato per l'intelligenza artificiale di cui all'articolo 56, atti di esecuzione secondo la procedura d'esame di cui all'articolo 74, paragrafo 2, che stabiliscono specifiche tecniche comuni per i requisiti di cui al capo 2 del presente titolo o, se del caso, dei requisiti di cui agli articoli 4 bis e 4 ter, se sono soddisfatte le seguenti condizioni:

   a) nessun riferimento a norme armonizzate che contemplano le pertinenti preoccupazioni essenziali in materia di sicurezza o di diritti fondamentali è pubblicato nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n. 1025/2012;

   b) a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, la Commissione ha chiesto a una o più organizzazioni europee di normazione di elaborare una norma armonizzata per i requisiti di cui al capo 2 del presente titolo;

   c) la richiesta di cui alla lettera b) non è stata accettata da nessuna delle organizzazioni europee di normazione o le norme armonizzate relative a tale richiesta non sono presentate entro il termine fissato a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012 o tali norme non sono conformi alla richiesta.

1 bis. Prima di preparare un progetto di atto di esecuzione, la Commissione informa il comitato di cui all'articolo 22 del regolamento (UE) n. 1025/2012 di ritenere soddisfatte le condizioni di cui al paragrafo 1.

2. Nella fase precoce dell'elaborazione del progetto di atto di esecuzione che stabilisce la specifica comune, la Commissione soddisfa gli obiettivi di cui all'articolo 40, paragrafo 2, e raccoglie i pareri dei pertinenti organismi o gruppi di esperti istituiti a norma del pertinente diritto settoriale dell'Unione. Sulla base di tale consultazione, la Commissione elabora il progetto di atto di esecuzione.

3. I sistemi di IA ad alto rischio o i sistemi di IA per finalità generali che sono conformi alle specifiche comuni di cui al paragrafo 1 si presumono conformi ai requisiti di cui al capo 2 del presente titolo o, se del caso, ai requisiti di cui agli articoli 4 bis e 4 ter, nella misura in cui tali requisiti sono contemplati da tali specifiche comuni.

4. Quando i riferimenti di una norma armonizzata sono pubblicati nella *Gazzetta ufficiale dell'Unione europea*, gli atti di esecuzione di cui al paragrafo 1, che contemplano i requisiti di cui al capo 2 del presente titolo o i requisiti di cui agli articoli 4 bis e 4 ter, sono abrogati, a seconda dei casi.

5. Se uno Stato membro ritiene che una specifica comune non soddisfi interamente i requisiti di cui al capo 2 del presente titolo o i requisiti di cui agli articoli 4 bis e 4 ter, a seconda dei casi, ne informa la Commissione fornendo una spiegazione dettagliata e la Commissione valuta tali informazioni e, ove necessario, modifica l'atto di esecuzione che stabilisce la specifica comune in questione.

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 o funzionale specifico all'interno del quale sono destinati a essere usati si presumono conformi ai rispettivi requisiti di cui all'articolo 10, paragrafo 4.

2. I sistemi di IA ad alto rischio o i sistemi di IA per finalità generali 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 del Parlamento europeo e del Consiglio[33] 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.

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 al capo 2 del presente titolo, il fornitore sceglie una delle procedure seguenti:

   a) la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI; oppure

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

   Se non ha applicato o ha applicato solo in parte le norme armonizzate di cui all'articolo 40 nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo 2 del presente titolo, o se tali norme armonizzate non esistono e non sono disponibili le specifiche comuni di cui all'articolo 41, il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII.

[33] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

Ai fini della procedura di valutazione della conformità di cui all'allegato VII, il fornitore può scegliere uno qualsiasi degli organismi notificati. Tuttavia, quando il sistema è destinato ad essere messo in servizio dalle autorità di contrasto, dalle autorità competenti in materia di immigrazione o di asilo, nonché da istituzioni, organi od organismi dell'UE, l'autorità di vigilanza del mercato di cui all'articolo 63, paragrafo 5 o 6, 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 e per i sistemi di IA per finalità generali di cui al titolo 1 bis, 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 ai quali si applicano gli atti giuridici elencati nell'allegato II, sezione A, il fornitore segue la pertinente valutazione della conformità prevista da tali atti giuridici. I requisiti di cui al capo 2 del presente titolo si applicano a tali sistemi di IA ad alto rischio e fanno parte di tale valutazione. Si applicano anche i punti 4.3, 4.4, 4.5 e il punto 4.6, quinto comma, dell'allegato VII.

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 rischio ai requisiti di cui al capo 2 del presente titolo, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 33, paragrafi 4, 9 e 10, sia stata valutata nel contesto della procedura di notifica a norma di tali atti giuridici.

Qualora gli atti giuridici elencati nell'allegato II, sezione A, consentano al fabbricante del prodotto di sottrarsi a una valutazione della conformità da 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 comuni di cui all'articolo 41, che contemplano i requisiti di cui al capo 2 del presente titolo.

4. [soppresso]

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare gli allegati VI e VII alla luce del progresso tecnico.

6. Alla Commissione è conferito il potere di adottare atti delegati al fine di modificare i paragrafi 1 e 2 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

1. I certificati rilasciati dagli organismi notificati a norma dell'allegato VII sono redatti in una lingua dell'Unione che può essere facilmente compresa dalle autorità pertinenti dello Stato membro in cui è stabilito l'organismo notificato.

2. I certificati sono validi per il periodo in essi indicato, che non può superare i cinque anni. Su domanda del fornitore, la validità di un certificato può essere prorogata per ulteriori periodi, ciascuno non superiore a cinque anni, sulla base di una nuova valutazione secondo le procedure di valutazione della conformità applicabili. Ogni integrazione del certificato rimane valida finché è valido il certificato cui si riferisce.

3. Qualora constati che il sistema di IA non soddisfa più i requisiti di cui al capo 2 del presente titolo, l'organismo notificato, tenendo conto del principio di proporzionalità, sospende o ritira il certificato rilasciato o impone limitazioni, a meno che la conformità a tali requisiti sia garantita mediante opportune misure correttive adottate dal fornitore del sistema entro un termine adeguato stabilito dall'organismo notificato. L'organismo notificato motiva la propria decisione.

Articolo 45

Ricorso contro le decisioni degli organismi notificati

È disponibile una procedura di ricorso contro le decisioni degli organismi notificati.

Articolo 46

Obblighi di informazione degli organismi notificati

1. Gli organismi notificati informano l'autorità di notifica in merito a quanto segue:

   a) i certificati di valutazione della documentazione tecnica dell'Unione, i supplementi a tali certificati e le approvazioni dei sistemi di gestione della qualità rilasciati in conformità ai requisiti dell'allegato VII;

   b) qualsiasi rifiuto, limitazione, sospensione o ritiro di un certificato di valutazione della documentazione tecnica dell'Unione o un'approvazione del sistema di gestione della qualità rilasciati in conformità ai requisiti dell'allegato VII;

   c) qualsiasi circostanza che influisca sull'ambito o sulle condizioni della notifica;

   d) qualsiasi richiesta di informazioni che hanno ricevuto dalle autorità di vigilanza del mercato, in relazione ad attività di valutazione della conformità;

   e) su richiesta, le attività di valutazione della conformità effettuate nell'ambito della loro notifica e qualsiasi altra attività, incluse quelle transfrontaliere e il subappalto.

2. Ciascun organismo notificato informa gli altri organismi notificati in merito a quanto segue:

   a) le approvazioni dei sistemi di gestione della qualità da esso rifiutate, sospese o ritirate e, su richiesta, le approvazioni dei sistemi di qualità da esso rilasciate;

b) i certificati di valutazione della documentazione tecnica dell'UE o i relativi supplementi da esso rifiutati, ritirati, sospesi o altrimenti limitati e, su richiesta, i certificati e/o i relativi supplementi da esso rilasciati.

3. Ciascun organismo notificato fornisce agli altri organismi notificati che svolgono attività simili di valutazione della conformità riguardanti gli stessi sistemi di IA informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, positivi della valutazione della conformità.

4. Gli obblighi di cui ai paragrafi da 1 a 3 sono rispettati in conformità dell'articolo 70.

Articolo 47

Deroga alla procedura di valutazione della conformità

1. In deroga all'articolo 43 e su richiesta debitamente giustificata, qualsiasi autorità di vigilanza del mercato può autorizzare l'immissione sul mercato o la messa in servizio di specifici sistemi di IA ad alto rischio nel territorio dello Stato membro interessato, per motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente e dei principali beni industriali e infrastrutturali. Tale autorizzazione è valida per un periodo di tempo limitato, mentre sono in corso le necessarie procedure di valutazione della conformità, e termina una volta completate tali procedure, tenendo conto dei motivi eccezionali che giustificano la deroga. Il completamento di tali procedure è effettuato senza indebito ritardo.

1 bis. In una situazione di urgenza debitamente giustificata per motivi eccezionali di sicurezza pubblica o in caso di minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche, le autorità di contrasto o le autorità di protezione civile possono mettere in servizio uno specifico sistema di IA ad alto rischio senza l'autorizzazione di cui al paragrafo 1, a condizione che tale autorizzazione sia richiesta durante o dopo l'uso senza indebito ritardo e che, se tale autorizzazione è rifiutata, l'utilizzo del sistema sia interrotto con effetto immediato e tutti i risultati e gli output di tale uso siano immediatamente abbandonati.

2. L'autorizzazione di cui al paragrafo 1 è rilasciata solo se l'autorità di vigilanza del mercato conclude che il sistema di IA ad alto rischio è conforme ai requisiti di cui al capo 2 del presente titolo. L'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri di eventuali autorizzazioni rilasciate a norma del paragrafo 1. Tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità di contrasto.

3. [soppresso]

4. [soppresso]

5. [soppresso]

6. Per i sistemi di IA ad alto rischio relativi ai prodotti contemplati dalla normativa di armonizzazione dell'Unione di cui all'allegato II, sezione A, si applicano solo le procedure di deroga per la valutazione della conformità stabilite in tale normativa.

Articolo 48

Dichiarazione di conformità UE

1. Il fornitore compila una dichiarazione, scritta o firmata elettronicamente, di conformità UE per ciascun sistema di IA e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA è stato immesso sul mercato. La dichiarazione di conformità UE identifica il sistema di IA per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti.

2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio in questione soddisfa i requisiti di cui al capo 2 del presente titolo. La dichiarazione di conformità UE riporta le informazioni di cui all'allegato V ed è tradotta in una lingua che può essere facilmente compresa dalle autorità nazionali competenti dello Stato membro o degli Stati membri nel quale il sistema di IA ad alto rischio è messo a disposizione.

3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altre normative di armonizzazione dell'Unione che richiedano anch'esse una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in relazione a tutte le normative dell'Unione applicabili al sistema di IA ad alto rischio. La dichiarazione contiene tutte le informazioni necessarie per identificare la normativa di armonizzazione dell'Unione cui si riferisce la dichiarazione.

4. Redigendo la dichiarazione di conformità UE, il fornitore si assume la responsabilità della conformità ai requisiti di cui al capo 2 del presente titolo. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 73 al fine di aggiornare il contenuto della dichiarazione di conformità UE di cui all'allegato V per introdurre elementi che si rendano necessari alla luce del progresso tecnico.

Articolo 49

Marcatura CE di conformità

1. La marcatura CE di conformità è soggetta ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

2. La marcatura CE è apposta sul sistema di IA ad alto rischio in modo visibile, leggibile e indelebile. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del sistema di IA ad alto rischio, il marchio è apposto sull'imballaggio o sui documenti di accompagnamento, a seconda dei casi.

3. Ove applicabile, la marcatura CE è seguita dal numero di identificazione dell'organismo notificato responsabile delle procedure di valutazione della conformità di cui all'articolo 43. Il numero d'identificazione è inoltre indicato in tutto il materiale promozionale in cui si afferma che il sistema di IA ad alto rischio soddisfa i requisiti per la marcatura CE.

Articolo 50

[soppresso]

Articolo 51

Registrazione degli operatori pertinenti e dei sistemi di IA ad alto rischio elencati nell'allegato III

1. Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della gestione della migrazione, dell'asilo e del controllo delle frontiere e dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, il fornitore e, se del caso, il rappresentante autorizzato si registrano nella banca dati dell'UE di cui all'articolo 60. Il fornitore o, se del caso, il rappresentante autorizzato registra anche i propri sistemi in tale banca dati.

2. Prima di utilizzare un sistema di IA ad alto rischio elencato nell'allegato III, gli utenti di sistemi di IA ad alto rischio che sono autorità, agenzie o organismi pubblici, o entità che agiscono per loro conto, si registrano nella banca dati dell'UE di cui all'articolo 60 e selezionano il sistema che intendono utilizzare.

   Gli obblighi di cui al comma precedente non si applicano alle autorità, alle agenzie o agli organismi di contrasto o competenti in materia di controllo delle frontiere, di immigrazione o di asilo e alle autorità, alle agenzie o agli organismi che utilizzano i sistemi di IA ad alto rischio di cui all'allegato III, punto 2, né alle entità che agiscono per loro conto.

TITOLO IV

OBBLIGHI DI TRASPARENZA PER I FORNITORI E GLI UTENTI DI DETERMINATI SISTEMI DI IA

Articolo 52

Obblighi di trasparenza per i fornitori e gli utenti di determinati sistemi di IA

1. I fornitori garantiscono che i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche 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 e 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. Gli utenti di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica autorizzati dalla legge per accertare, prevenire e indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

2 bis. Gli utenti di un sistema di riconoscimento delle emozioni informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema. Tale obbligo non si applica ai sistemi di IA utilizzati per il riconoscimento delle emozioni autorizzati dalla legge per accertare, prevenire e indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

3. Gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente.

Tuttavia, il primo comma non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare e perseguire reati o se il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico o fittizio, fatte salve le tutele adeguate per i diritti e le libertà dei terzi.

3 bis. Le informazioni di cui ai paragrafi da 1 a 3 sono fornite alle persone fisiche in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione.

4. I paragrafi 1, 2, 2 bis, 3 e 3 bis lasciano impregiudicati i requisiti e gli obblighi di cui al titolo III del presente regolamento, così come gli altri obblighi di trasparenza per gli utenti di sistemi di IA stabiliti dal diritto dell'Unione o nazionale.

TITOLO V

MISURE A SOSTEGNO DELL'INNOVAZIONE

Articolo 53

Spazi di sperimentazione normativa per l'IA

-1 bis. Le autorità nazionali competenti possono istituire spazi di sperimentazione normativa per l'IA per lo sviluppo, l'addestramento, le prove e la convalida di sistemi di IA innovativi sotto la guida, il controllo e il sostegno diretti dell'autorità nazionale competente, prima che tali sistemi siano immessi sul mercato o messi in servizio. Tali spazi di sperimentazione normativa possono comprendere prove in condizioni reali sotto il controllo delle autorità nazionali competenti.

-1 ter. [soppresso]

-1 quater. 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.

-1 quinquies. Il presente articolo lascia impregiudicati gli altri spazi di sperimentazione normativa istituiti a norma del diritto nazionale o dell'Unione, anche nei casi in cui i prodotti o i servizi che vi sono sottoposti a prova siano collegati all'uso di sistemi di IA innovativi. Gli Stati membri garantiscono un livello adeguato di cooperazione tra le autorità che controllano tali altri spazi di sperimentazione e le autorità nazionali competenti.

1. [soppresso]

1 bis. [soppresso]

1 ter. L'istituzione di spazi di sperimentazione normativa per l'IA a norma del presente regolamento mira a contribuire a uno o più dei seguenti obiettivi:

a) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA;
b) agevolare e accelerare l'accesso al mercato dell'Unione per i sistemi di IA, in particolare se forniti dalle piccole e medie imprese (PMI), comprese le start-up;
c) migliorare la certezza del diritto e contribuire alla condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA al fine di garantire la futura conformità al presente regolamento e, se del caso, ad altre normative dell'Unione e degli Stati membri;
d) contribuire all'apprendimento normativo basato su dati concreti.

2. [soppresso]

2 bis. L'accesso agli spazi di sperimentazione normativa per l'IA è aperto a qualsiasi fornitore o potenziale fornitore di un sistema di IA che soddisfi i criteri di ammissibilità e selezione di cui al paragrafo 6, lettera a), e che sia stato selezionato dalle autorità nazionali competenti a seguito della procedura di selezione di cui al paragrafo 6, lettera b). I fornitori o potenziali fornitori possono anche presentare domande in partenariato con gli utenti o con altri terzi interessati.

La partecipazione allo spazio di sperimentazione normativa per l'IA è limitata a un periodo adeguato alla complessità e alla portata del progetto. Tale periodo può essere prorogato dall'autorità nazionale competente.

La partecipazione allo spazio di sperimentazione normativa per l'IA si basa su un piano specifico di cui al paragrafo 6 che è concordato tra i partecipanti e le autorità nazionali competenti, a seconda dei casi.

3. La partecipazione agli spazi di sperimentazione normativa per l'IA non pregiudica i poteri correttivi e di controllo delle autorità che controllano tali spazi. Tali autorità esercitano i loro poteri di controllo in modo flessibile entro i limiti della legislazione pertinente, utilizzando i loro poteri discrezionali nell'attuazione delle disposizioni giuridiche per uno specifico progetto di spazio di sperimentazione per l'IA, con l'obiettivo di sostenere l'innovazione nell'IA nell'Unione.

A condizione che i partecipanti rispettino il piano dello spazio di sperimentazione e i termini e le condizioni di partecipazione di cui al paragrafo 6, lettera c), e seguano in buona fede gli orientamenti forniti dalle autorità, queste ultime non impongono alcuna sanzione amministrativa pecuniaria per violazione della normativa applicabile dell'Unione o degli Stati membri relativa al sistema di IA controllato nello spazio di sperimentazione, comprese le disposizioni del presente regolamento.

4. I partecipanti restano responsabili ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni causati nel corso della loro partecipazione a uno spazio di sperimentazione normativa per l'IA.

4 bis. Su richiesta del fornitore o potenziale fornitore del sistema di IA, l'autorità nazionale competente fornisce, se del caso, una prova scritta delle attività svolte con successo nello spazio di sperimentazione. L'autorità nazionale competente fornisce inoltre una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione e i relativi risultati e conclusioni dell'apprendimento. La prova scritta e la relazione di uscita potrebbero essere prese in considerazione dalle autorità di vigilanza del mercato o dagli organismi notificati, a seconda dei casi, nel contesto delle procedure di valutazione della conformità o dei controlli di vigilanza del mercato.

Fatte salve le disposizioni in materia di riservatezza di cui all'articolo 70 e con l'accordo dei partecipanti allo spazio di sperimentazione, la Commissione europea e il comitato per l'intelligenza artificiale 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 partecipante che l'autorità nazionale competente vi acconsentono esplicitamente, la relazione di uscita può essere messa a disposizione del pubblico attraverso la piattaforma unica di informazione di cui all'articolo 55, paragrafo 3, lettera b).

4 ter. 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.

5. Le autorità nazionali competenti mettono pubblicamente a disposizione le relazioni annuali sull'attuazione degli spazi di sperimentazione normativa per l'IA, comprese le buone pratiche, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione del presente regolamento e di altre normative dell'Unione soggette a controllo nell'ambito dello spazio di sperimentazione. Tali relazioni annuali sono presentate al comitato per l'intelligenza artificiale, che mette a disposizione del pubblico una sintesi di tutti gli insegnamenti tratti, le buone pratiche e le raccomandazioni. Tale obbligo di mettere le relazioni annuali a disposizione del pubblico non riguarda i dati operativi sensibili in relazione alle attività delle autorità di contrasto o competenti in materia di controllo delle frontiere, di immigrazione o di asilo. La Commissione e il comitato per l'intelligenza artificiale tengono conto, se del caso, delle relazioni annuali nell'esercizio dei loro compiti a norma del presente regolamento.

5 ter. La Commissione garantisce che le informazioni sugli spazi di sperimentazione normativa per l'IA, compresi quelli istituiti a norma del presente articolo, siano disponibili attraverso la piattaforma unica di informazione di cui all'articolo 55, paragrafo 3, lettera b).

6. Le modalità e le condizioni per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA a norma del presente regolamento sono adottate mediante atti di esecuzione secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Le modalità e le condizioni sostengono quanto più possibile la flessibilità che consente alle autorità nazionali competenti di istituire e gestire i loro spazi di sperimentazione normativa per l'IA, promuovono l'innovazione e l'apprendimento normativo e tengono conto segnatamente delle circostanze particolari e delle capacità delle PMI partecipanti, comprese le start-up.

Tali atti di esecuzione comprendono principi fondamentali comuni sulle questioni seguenti:

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

7. Quando valutano la possibilità di autorizzare prove in condizioni reali sottoposte a controllo nel quadro di uno spazio di sperimentazione normativa per l'IA istituito 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 54

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 ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi alle seguenti condizioni cumulative:

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

      i) [soppresso]

      ii) la sicurezza pubblica e la sanità pubblica, compresi la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari;

      iii) la protezione e il miglioramento della qualità dell'ambiente, compresi la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi;

      iv) la sostenibilità energetica, i trasporti e la mobilità;

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

      vi) la cibersicurezza e la resilienza delle infrastrutture critiche.

   b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al titolo III, capo 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento anonimizzato, sintetico 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 dei partecipanti e solo le persone autorizzate hanno accesso a tali dati;

e) i dati personali trattati non devono essere trasmessi, trasferiti o altrimenti consultati da terzi che non partecipano allo spazio di sperimentazione, a meno che tale divulgazione avvenga in conformità del regolamento (UE) 2016/679 o, se del caso, del regolamento (UE) 2018/1725 e tutti i partecipanti vi abbiano acconsentito;

f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non pregiudica l'applicazione dei diritti degli interessati previsti dal diritto dell'Unione in materia di protezione dei dati personali, in particolare dall'articolo 22 del regolamento (UE) 2016/679 e dall'articolo 24 del regolamento (UE) 2018/1725;

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 di contrasto o in materia di controllo delle frontiere, di immigrazione o di asilo.

1 bis. 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 sul diritto di uno specifico Stato membro o sul diritto dell'Unione e è soggetto alle stesse condizioni cumulative di cui al paragrafo 1.

2. Il paragrafo 1 lascia impregiudicato il diritto dell'Unione o degli Stati membri 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.

Articolo 54 bis

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 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, conformemente alle disposizioni del presente articolo e al piano di prova in condizioni reali di cui al presente articolo.

Gli elementi dettagliati del piano di prova in condizioni reali sono specificati negli atti di esecuzione adottati dalla Commissione secondo la procedura d'esame di cui all'articolo 74, paragrafo 2.

Tale disposizione lascia impregiudicata la normativa dell'Unione o degli Stati membri concernente le prove in condizioni reali di sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di cui all'allegato II.

2. I fornitori o potenziali fornitori possono effettuare prove dei sistemi di IA ad alto rischio di cui all'allegato III in condizioni reali in qualsiasi momento prima dell'immissione sul mercato o della messa in servizio del sistema di IA, da soli o in partenariato con uno o più potenziali utenti.

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

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

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 o degli Stati membri in cui devono essere effettuate le prove in condizioni reali;

b) l'autorità di vigilanza del mercato dello Stato membro o degli Stati membri in cui devono essere effettuate le prove in condizioni reali non ha sollevato obiezioni in merito alle prove entro 30 giorni dalla presentazione del piano di prova;

c) il fornitore o potenziale fornitore, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della gestione della migrazione, dell'asilo e 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 nella banca dati dell'UE di cui all'articolo 60, paragrafo 5 bis, con un numero di identificazione unico a livello dell'Unione, come anche le informazioni di cui all'allegato VIII bis;

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

e) i dati raccolti e trattati ai fini delle prove in condizioni reali non sono trasferiti a paesi al di fuori dell'Unione, a meno che il trasferimento e il trattamento non offrano tutele equivalenti a quelle previste dal diritto dell'Unione;

f) le prove in condizioni reali non durano più di quanto necessario per il conseguimento dei loro obiettivi e in ogni caso non oltre 12 mesi;

g) le persone appartenenti a gruppi vulnerabili a causa della loro età o disabilità fisica o mentale sono adeguatamente protette;

h) [soppresso]

i) qualora un fornitore o potenziale fornitore organizzi le prove in condizioni reali in cooperazione con uno o più potenziali utenti, questi ultimi sono stati informati di tutti gli aspetti delle prove pertinenti per la loro decisione di partecipare e hanno ricevuto le istruzioni pertinenti su come utilizzare il sistema di IA di cui all'articolo 13; il fornitore o potenziale fornitore e l'utente o gli utenti 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 normative applicabili dell'Unione e degli Stati membri;

j) i soggetti delle prove in condizioni reali hanno dato il proprio consenso informato a norma dell'articolo 54 ter 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 un effetto negativo sul soggetto;

k) le prove in condizioni reali sono efficacemente supervisionate dal fornitore o potenziale fornitore e utente o utenti con persone adeguatamente qualificate nel settore pertinente e dotate delle capacità, della formazione e dell'autorità necessarie per svolgere i loro compiti;

l) le previsioni, le raccomandazioni o le decisioni del sistema di IA possono essere efficacemente ribaltate o 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. La revoca del consenso informato non pregiudica le attività già svolte e l'uso dei dati ottenuti sulla base del consenso informato prima della revoca.

6. Qualsiasi incidente grave individuato nel corso delle prove in condizioni reali è segnalato all'autorità nazionale di vigilanza del mercato conformemente all'articolo 62 del presente regolamento. 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.

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

8. Il fornitore o potenziale fornitore è responsabile ai sensi della normativa applicabile dell'Unione e degli Stati membri in materia di responsabilità per eventuali danni causati nel corso della sua partecipazione alle prove in condizioni reali.

Articolo 54 ter

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

1. Ai fini delle prove in condizioni reali di cui all'articolo 54 bis, il consenso informato è dato liberamente dal soggetto delle prove prima della sua partecipazione a tali prove e dopo essere stato debitamente informato con indicazioni concise, chiare, pertinenti e comprensibili riguardanti:

i) la natura e gli obiettivi delle prove in condizioni reali e i possibili disagi che possono essere connessi alla sua partecipazione;

ii) le condizioni alle quali devono essere effettuate le prove in condizioni reali, compresa la durata prevista della partecipazione del soggetto;

iii) i diritti e le garanzie riconosciuti al soggetto in relazione alla sua partecipazione, in particolare il suo diritto di rifiutarsi di partecipare e il diritto di ritirarsi dalle prove in condizioni reali in qualsiasi momento, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione;

iv) le modalità per richiedere che le previsioni, raccomandazioni o decisioni del sistema di IA siano ignorate o ribaltate;

v) il numero di identificazione unico a livello dell'Unione delle prove in condizioni reali conformemente all'articolo 54 bis, paragrafo 4 quater, e i dati di contatto del fornitore o del suo rappresentante legale da cui è possibile ottenere ulteriori informazioni.

2. Il consenso informato è datato e documentato e una copia è consegnata al soggetto o al suo rappresentante legale.

Articolo 55

Misure di sostegno per gli operatori, in particolare per le PMI, comprese le start-up

1. Gli Stati membri intraprendono le seguenti azioni:

a) fornire alle PMI, comprese le start-up, un accesso prioritario agli spazi di sperimentazione normativa per l'IA nella misura in cui soddisfano i criteri di ammissibilità e selezione;

b) organizzare specifiche attività di sensibilizzazione e formazione sull'applicazione del presente regolamento adattate alle esigenze delle PMI, comprese le start-up e, se del caso, delle autorità pubbliche locali;

c) ove opportuno, istituire un canale dedicato per la comunicazione con le PMI, comprese le start-up e, se del caso, le autorità pubbliche locali, al fine di fornire consulenza e rispondere alle domande sull'attuazione del presente regolamento, anche per quanto riguarda la partecipazione agli spazi di sperimentazione normativa per l'IA.

2. Nel fissare le tariffe per la valutazione della conformità a norma dell'articolo 43 si tiene conto degli interessi e delle esigenze specifici delle PMI fornitrici, comprese le start-up, riducendo tali tariffe proporzionalmente alle loro dimensioni, alle dimensioni del loro mercato e ad altri indicatori pertinenti.

3. La Commissione intraprende le azioni seguenti:

su richiesta del comitato per l'intelligenza artificiale, fornire modelli standardizzati per i settori disciplinati dal presente regolamento;

sviluppare e mantenere una piattaforma unica di informazione che fornisce informazioni di facile uso in relazione al presente regolamento per tutti gli operatori in tutta l'Unione;

organizzare adeguate campagne di comunicazione per sensibilizzare in merito agli obblighi derivanti dal presente regolamento;

valutare e promuovere la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA.

Articolo 55 bis

Deroghe per operatori specifici

1. Gli obblighi di cui all'articolo 17 del presente regolamento non si applicano alle microimprese quali definite all'articolo 2, paragrafo 3, dell'allegato della raccomandazione 2003/361/CE della Commissione relativa alla definizione delle microimprese, piccole e medie imprese, purché tali imprese non abbiano imprese associate o collegate quali definite all'articolo 3 dello stesso allegato.

2. Il paragrafo 1 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, 61 e 62.

3. I requisiti e gli obblighi per i sistemi di IA per finalità generali di cui all'articolo 4 ter non si applicano alle microimprese e alle piccole e medie imprese, purché tali imprese non abbiano imprese associate o collegate quali definite all'articolo 3 dell'allegato della raccomandazione 2003/361/CE della Commissione relativa alla definizione delle microimprese, piccole e medie imprese.

TITOLO VI

GOVERNANCE

CAPO 1

COMITATO EUROPEO PER L'INTELLIGENZA ARTIFICIALE

Articolo 56

Istituzione e struttura del comitato europeo per l'intelligenza artificiale

1. È istituito un "comitato europeo per l'intelligenza artificiale" (il "comitato").

2. Il comitato è composto di un rappresentante per Stato membro. Il Garante europeo della protezione dei dati partecipa come osservatore. Anche la Commissione partecipa alle riunioni del comitato senza partecipare alle votazioni.

   Altre autorità, organismi o esperti nazionali e dell'Unione possono essere invitati alle riunioni dal comitato caso per caso, qualora le questioni discusse siano di loro pertinenza.

2 bis. Ciascun rappresentante è designato dal rispettivo Stato membro per un periodo di tre anni, rinnovabile una volta.

2 bis bis. Gli Stati membri provvedono affinché i loro rappresentanti nel comitato:

   i) dispongano delle competenze e dei poteri pertinenti nel proprio Stato membro in modo da contribuire attivamente allo svolgimento dei compiti del comitato di cui all'articolo 58;

   ii) siano designati come punto di contatto unico nei confronti del comitato e, se del caso tenendo conto delle esigenze degli Stati membri, come punto di contatto unico per i portatori di interessi;

iii) abbiano il potere di agevolare la coerenza e il coordinamento tra le autorità nazionali competenti nel rispettivo Stato membro per quanto riguarda l'attuazione del presente regolamento, anche attraverso la raccolta di dati e informazioni pertinenti ai fini dello svolgimento dei loro compiti in seno al comitato.

3. I rappresentanti designati degli Stati membri adottano il regolamento interno del comitato a maggioranza di due terzi.

Il regolamento interno stabilisce, in particolare, le procedure per il processo di selezione, la durata del mandato e le specifiche riguardanti i compiti del presidente, le modalità di voto e l'organizzazione delle attività del comitato e dei suoi sottogruppi.

Il comitato istituisce un sottogruppo permanente che funge da piattaforma per i portatori di interessi con il compito di fornire consulenza al comitato su tutte le questioni connesse all'attuazione del presente regolamento, compresa l'elaborazione di atti di esecuzione e atti delegati. A tal fine, sono invitati a partecipare a tale sottogruppo le organizzazioni che rappresentano gli interessi dei fornitori e degli utenti dei sistemi di IA, comprese le PMI e le start-up, nonché le organizzazioni della società civile, i rappresentanti delle persone interessate, i ricercatori, le organizzazioni di normazione, gli organismi notificati, i laboratori e gli impianti di prova e sperimentazione. Il comitato istituisce due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e le autorità di notifica su questioni relative rispettivamente alla vigilanza del mercato e agli organismi notificati.

Il comitato può istituire altri sottogruppi permanenti o temporanei, se del caso, ai fini dell'esame di questioni specifiche. Se del caso, i portatori di interessi di cui al comma precedente possono essere invitati a tali sottogruppi o a riunioni specifiche di tali sottogruppi in qualità di osservatori.

3 bis. Il comitato è organizzato e gestito in modo che sia salvaguardata l'obiettività e l'imparzialità delle sue attività.

4. Il comitato è presieduto da uno dei rappresentanti degli Stati membri. Su richiesta della presidenza, la Commissione convoca le riunioni e prepara l'ordine del giorno in conformità dei compiti del comitato a norma del presente regolamento e del relativo regolamento interno. La Commissione fornisce sostegno amministrativo e analitico per le attività del comitato a norma del presente regolamento.

Articolo 57

[soppresso]

Articolo 58

Compiti del comitato

Il comitato fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del presente regolamento. A tal fine il comitato può in particolare:

a) raccogliere e condividere tra gli Stati membri conoscenze e migliori pratiche tecniche e normative;

b) contribuire all'armonizzazione delle pratiche amministrative negli Stati membri, anche in relazione alla deroga alle procedure di valutazione della conformità di cui all'articolo 47, al funzionamento degli spazi di sperimentazione normativa e alle prove in condizioni reali di cui agli articoli 53, 54 e 54 bis;

c) su richiesta della Commissione o di propria iniziativa, formulare raccomandazioni e pareri scritti su qualsiasi questione pertinente relativa all'attuazione del presente regolamento e alla sua applicazione coerente ed efficace, tra l'altro:

   i) sulle specifiche tecniche o sulle norme esistenti relative ai requisiti di cui al titolo III, capo 2,

   ii) sull'uso delle norme armonizzate o delle specifiche comuni di cui agli articoli 40 e 41,

iii) sulla preparazione di documenti di orientamento, compresi gli orientamenti per stabilire le sanzioni amministrative pecuniarie di cui all'articolo 71;

d) fornire consulenza alla Commissione sull'eventuale necessità di modificare l'allegato III conformemente agli articoli 4 e 7, tenendo conto delle pertinenti prove disponibili e degli ultimi sviluppi tecnologici;

e) fornire consulenza alla Commissione durante la preparazione di atti di esecuzione o di atti delegati a norma del presente regolamento;

f) cooperare, se del caso, con i pertinenti organismi, gruppi di esperti e reti dell'UE, in particolare nei settori della sicurezza dei prodotti, della cibersicurezza, della concorrenza, dei servizi digitali e dei media, dei servizi finanziari, delle criptovalute, della protezione dei consumatori, dei dati e dei diritti fondamentali;

g) contribuire e fornire consulenza pertinente alla Commissione nell'elaborazione degli orientamenti di cui all'articolo 58 bis o chiedere l'elaborazione di tali orientamenti;

h) assistere le autorità di vigilanza del mercato e, in cooperazione e previo accordo delle autorità di vigilanza del mercato interessate, promuovere e sostenere le indagini transfrontaliere di vigilanza del mercato, anche per quanto riguarda l'emergere di rischi di natura sistemica che possono derivare dai sistemi di IA;

i) contribuire alla valutazione delle esigenze di formazione del personale degli Stati membri coinvolto nell'attuazione del presente regolamento;

j) fornire consulenza alla Commissione sulle questioni internazionali in materia di intelligenza artificiale.

CAPO 1 BIS

ORIENTAMENTI DELLA COMMISSIONE

Articolo 58 bis

Orientamenti della Commissione sull'attuazione del regolamento

1. Su richiesta degli Stati membri o del comitato, o di propria iniziativa, la Commissione emana orientamenti sull'attuazione pratica del presente regolamento, in particolare per quanto riguarda:

   i) l'applicazione dei requisiti di cui agli articoli da 8 a 15;

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

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

   iv) l'attuazione pratica delle condizioni uniformi di cui all'articolo 6, paragrafo 3, compresi esempi relativi ai sistemi di IA ad alto rischio di cui all'allegato III;

   v) l'attuazione pratica degli obblighi di trasparenza di cui all'articolo 52;

   vi) la relazione del presente regolamento con altre normative pertinenti dell'Unione, anche per quanto riguarda la coerenza della loro applicazione.

Quando pubblica tali orientamenti, la Commissione presta particolare attenzione alle esigenze delle PMI, comprese le start-up, delle autorità pubbliche locali e dei settori maggiormente interessati dal presente regolamento.

CAPO 2

AUTORITÀ NAZIONALI COMPETENTI

Articolo 59

Designazione delle autorità nazionali competenti

1. [soppresso]

2. 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. Queste autorità nazionali competenti sono organizzate in modo che siano salvaguardati i principi di obiettività e imparzialità dei loro compiti e delle loro attività. 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.

3. Gli Stati membri informano la Commissione della loro designazione o delle loro designazioni.

4. Gli Stati membri garantiscono che le autorità nazionali competenti dispongano di risorse finanziarie, attrezzature tecniche e risorse umane qualificate adeguate per svolgere efficacemente i loro compiti a norma del presente regolamento.

5. Entro [*un anno dall'entrata in vigore del presente regolamento*] e successivamente sei mesi prima del termine di cui all'articolo 84, paragrafo 2, gli Stati membri informano la Commissione in merito allo stato delle risorse finanziarie, delle attrezzature tecniche e della risorse umane delle autorità nazionali competenti, con una valutazione della loro adeguatezza. La Commissione trasmette tali informazioni al comitato affinché le discuta e formuli eventuali raccomandazioni.

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

7. Le autorità nazionali competenti possono fornire consulenza riguardo all'attuazione del presente regolamento, fra cui consulenza mirata alle PMI fornitrici, comprese le start-up. Ogniqualvolta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre normative dell'Unione, sono consultate le autorità nazionali competenti a norma di tale normativa dell'Unione, come opportuno. Gli Stati membri possono inoltre istituire un punto di contatto centrale per la comunicazione con gli operatori.

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

TITOLO VII

BANCA DATI DELL'UE PER I SISTEMI DI IA AD ALTO RISCHIO ELENCATI NELL'ALLEGATO III

Articolo 60

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

1. La Commissione, in collaborazione con gli Stati membri, istituisce e mantiene una banca dati dell'UE contenente le informazioni di cui al paragrafo 2 relative agli operatori pertinenti e ai sistemi di IA ad alto rischio elencati nell'allegato III, registrati conformemente agli articoli 51 e 54 bis. Nel definire le specifiche funzionali di tale banca dati, la Commissione consulta il comitato per l'IA.

2. I dati elencati nell'allegato VIII, parte I, sono inseriti nella banca dati UE dai fornitori, dai rappresentanti autorizzati e dagli utenti pertinenti, a seconda dei casi, al momento della loro registrazione. I dati elencati nell'allegato VIII, parte II, punti da 1 a 11, sono inseriti nella banca dati UE dai fornitori o, se del caso, dal rappresentante autorizzato, conformemente all'articolo 51. I dati di cui all'allegato VIII, parte II, punto 12, sono generati automaticamente dalla banca dati sulla base delle informazioni fornite dagli utenti pertinenti a norma dell'articolo 51, paragrafo 2. I dati elencati nell'allegato VIII bis sono inseriti nella banca dati dai fornitori o potenziali fornitori a norma dell'articolo 54 bis.

3. [soppresso]

4. La banca dati dell'UE non contiene dati personali, ad eccezione delle informazioni elencate nell'allegato VIII, e lascia impregiudicato l'articolo 70.

5. La Commissione è il titolare del trattamento della banca dati dell'UE. Essa mette a disposizione dei fornitori, dei potenziali fornitori e degli utenti un adeguato sostegno tecnico e amministrativo.

5 bis. Le informazioni contenute nella banca dati dell'UE registrate ai sensi dell'articolo 51 sono accessibili al pubblico. Le informazioni registrate a norma dell'articolo 54 bis sono accessibili solo alle autorità di vigilanza del mercato e alla Commissione, a meno che il fornitore o il potenziale fornitore non abbia dato il suo consenso a rendere tali informazioni accessibili anche al pubblico.

TITOLO VIII

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

CAPO 1

MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO

Articolo 61

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 ai rischi del sistema di IA ad alto rischio.

2. Al fine di consentire al fornitore di valutare la conformità dei sistemi di IA ai requisiti di cui al titolo III, capo 2, durante l'intero ciclo di vita, il sistema di monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza i dati pertinenti sulle prestazioni dei sistemi di IA ad alto rischio che possono essere forniti dagli utenti o raccolti attraverso altre fonti. Tale obbligo non riguarda i dati operativi sensibili degli utenti dei sistemi di IA 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 adotta un atto di esecuzione che stabilisce disposizioni dettagliate in cui si definisce un modello per il piano di monitoraggio successivo all'immissione sul mercato e un elenco di elementi da includere nel piano.

4. Per i sistemi di IA ad alto rischio disciplinati dagli atti giuridici di cui all'allegato II, sezione A, qualora tale normativa preveda già un sistema e un piano di monitoraggio successivo all'immissione sul mercato, la documentazione relativa al monitoraggio successivo all'immissione sul mercato preparata in virtù di tale normativa è ritenuta sufficiente a condizione che sia utilizzato il modello di cui al paragrafo 3.

Il primo comma 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 che sono soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della normativa dell'Unione sui servizi finanziari.

CAPO 2

CONDIVISIONE DI INFORMAZIONI SU INCIDENTI GRAVI

Articolo 62

Comunicazione di incidenti gravi

1. I fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti si sono verificati.

Tale notifica è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente grave o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che è venuto a conoscenza dell'incidente grave.

2. Al ricevimento di una notifica relativa a un incidente grave di cui all'articolo 3, punto 44, lettera c), l'autorità di vigilanza del mercato interessata informa le autorità o gli organismi pubblici nazionali di cui all'articolo 64, paragrafo 3. La Commissione elabora orientamenti specifici per facilitare il rispetto degli obblighi di cui al paragrafo 1. Tali orientamenti sono emanati al più tardi 12 mesi dopo l'entrata in vigore del presente regolamento.

3. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 5, immessi sul mercato o messi in servizio da fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma della normativa dell'Unione sui servizi finanziari, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 44, lettera c).

4. Per i sistemi di IA ad alto rischio che sono componenti di sicurezza di dispositivi, o sono essi stessi dispositivi, disciplinati dal regolamento (EU) 2017/745 e dal regolamento (UE) 2017/746, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 44, lettera c) ed è trasmessa all'autorità nazionale competente scelta a tal fine dagli Stati membri in cui si è verificato l'incidente.

CAPO 3

APPLICAZIONE

Articolo 63

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

1. Il regolamento (UE) 2019/1020 si applica ai sistemi di IA disciplinati dal presente regolamento. Tuttavia, ai fini dell'efficace applicazione del presente regolamento:

   a) ogni riferimento a un operatore economico a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti gli operatori di cui all'articolo 2 del presente regolamento;

   b) ogni riferimento a un prodotto a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti i sistemi di IA che rientrano nell'ambito di applicazione del presente regolamento.

2. Nell'ambito dei loro obblighi in materia di segnalazione a norma dell'articolo 34, paragrafo 4, del regolamento (UE) 2019/1020, le autorità di vigilanza del mercato riferiscono alla Commissione in merito ai risultati delle pertinenti attività di vigilanza del mercato a norma del presente regolamento.

3. Per i sistemi di IA ad alto rischio, collegati a prodotti cui si applicano gli atti giuridici elencati nell'allegato II, sezione A, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità responsabile delle attività di vigilanza del mercato designata a norma di tali atti giuridici o, in casi giustificati e a condizione che sia garantito il coordinamento, un'altra autorità pertinente individuata dallo Stato membro.

Le procedure di cui agli articoli 65, 66, 67 e 68 del presente regolamento non si applicano ai sistemi di IA collegati a prodotti ai quali si applicano gli atti giuridici elencati nell'allegato II, sezione A, qualora tali atti giuridici prevedano già procedure aventi lo stesso obiettivo. In tal caso si applicano dette procedure settoriali.

4. Per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dalla normativa dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale normativa, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di tali servizi finanziari.

In deroga al comma precedente, in casi giustificati e a condizione che sia garantito il coordinamento, lo Stato membro può individuare un'altra autorità competente come autorità di vigilanza del mercato ai fini del presente regolamento.

Le autorità nazionali di vigilanza del mercato che controllano gli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento n. 1204/2013 del Consiglio, dovrebbero comunicare senza indugio alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento.

5. Per i sistemi di IA ad alto rischio elencati al punto 1, lettera a), nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, e ai punti 6, 7 e 8 dell'allegato III, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità nazionali che controllano le attività delle autorità di contrasto o delle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo, o le autorità giudiziarie o le autorità di controllo competenti per la protezione dei dati a norma della direttiva (UE) 2016/680 o del regolamento (CE) n. 2016/679. Le attività di vigilanza del mercato non pregiudicano in alcun modo l'indipendenza delle autorità giudiziarie né interferiscono in altro modo con le loro attività nell'esercizio delle loro funzioni giurisdizionali.

6. Nei casi in cui le istituzioni, gli organi e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità di vigilanza del mercato.

7. Gli Stati membri agevolano il coordinamento tra le autorità di vigilanza del mercato designate a norma del presente regolamento e altre autorità o organismi nazionali pertinenti che controllano l'applicazione della normativa di armonizzazione dell'Unione elencata nell'allegato II o di altre normative dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III.

8. Fatti salvi i poteri di cui al regolamento (UE) 2019/1020 e se del caso e nei limiti di quanto necessario per lo svolgimento dei loro compiti, il fornitore concede alle autorità di vigilanza del mercato pieno accesso alla documentazione nonché ai set di dati di addestramento, convalida e prova utilizzati per lo sviluppo dei sistemi di IA ad alto rischio, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso interfacce di programmazione delle applicazioni (API) o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.

9. Alle autorità di vigilanza del mercato è concesso l'accesso al codice sorgente del sistema di IA ad alto rischio su richiesta motivata e solo qualora siano soddisfatte le seguenti condizioni cumulative:

a) l'accesso al codice sorgente è necessario per valutare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al titolo III, capo 2; e

b) le procedure di prova e di audit e le verifiche basate sui dati e sulla documentazione presentati dal fornitore sono state esaurite o si sono dimostrate insufficienti.

10. Qualsiasi informazione e documentazione ottenuta dalle autorità di vigilanza del mercato è trattata nel rispetto degli obblighi di riservatezza di cui all'articolo 70.

11. I reclami alla pertinente autorità di vigilanza del mercato possono essere presentati da qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del presente regolamento.

Conformemente all'articolo 11, paragrafo 3, lettera e), e all'articolo 11, paragrafo 7, lettera a), del regolamento (UE) 2019/1020, i reclami sono presi in considerazione ai fini dello svolgimento delle attività di vigilanza del mercato e sono trattati in linea con le procedure specifiche stabilite a tal fine dalle autorità di vigilanza del mercato.

Articolo 63 bis

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

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

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 54, le autorità di vigilanza del mercato verificano la conformità delle disposizioni dell'articolo 54 bis 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 54 bis, 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 54 bis e 54 ter 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 all'utente o agli utenti 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 54 bis, paragrafo 4, lettera b), la decisione o l'obiezione ne indica i motivi e le modalità e condizioni in base alle quali 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 64

Poteri delle autorità che tutelano i diritti fondamentali

1. [soppresso]

2. [soppresso]

3. 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, in relazione all'uso dei sistemi di IA ad alto rischio di cui all'allegato III hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi quando l'accesso a tale documentazione è necessario per l'adempimento delle competenze a norma del loro mandato entro i limiti della loro giurisdizione. L'autorità pubblica o l'organismo pubblico pertinente informa l'autorità di vigilanza del mercato dello Stato membro interessato di qualsiasi richiesta in tal senso.

4. Entro tre mesi dall'entrata in vigore del presente regolamento, ciascuno Stato membro individua le autorità o gli organismi pubblici di cui al paragrafo 3 e pubblica l'elenco. Gli Stati membri notificano l'elenco alla Commissione e a tutti gli altri Stati membri e lo tengono aggiornato.

5. Qualora la documentazione di cui al paragrafo 3 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 3 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.

6. Qualsiasi informazione e documentazione ottenuta dalle autorità o dagli organismi pubblici nazionali di cui al paragrafo 3 a norma delle disposizioni del presente articolo è trattata nel rispetto degli obblighi di riservatezza di cui all'articolo 70.

Articolo 65

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

1. Un sistema di IA che presenta un rischio è inteso come un prodotto che presenta un rischio definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 per quanto riguarda i rischi per la salute o la sicurezza o per i diritti fondamentali delle persone.

2. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia motivi sufficienti per ritenere che un sistema di IA presenti un rischio di cui al paragrafo 1, essa effettua una valutazione del sistema di IA interessato per quanto riguarda la sua conformità a tutti i requisiti e gli obblighi di cui al presente regolamento. Qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti di cui all'articolo 64, paragrafo 3. I pertinenti operatori cooperano, per quanto necessario, con le autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali di cui all'articolo 64, paragrafo 3.

   Se, nel corso di tale valutazione, le autorità di vigilanza del mercato rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza indebito ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di, a seconda dei casi, ripristinare la conformità del sistema di IA, ritirarlo dal mercato o richiamarlo entro il termine da esse prescritto.

   L'autorità di vigilanza del mercato informa di conseguenza l'organismo notificato pertinente. L'articolo 18 del regolamento (UE) 2019/1020 si applica alle misure di cui al secondo comma.

3. Qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri senza indebito ritardo dei risultati della valutazione e delle azioni che hanno chiesto all'operatore economico di intraprendere.

4. L'operatore garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato in tutta l'Unione.

5. Qualora l'operatore di un sistema di IA non adotti misure correttive adeguate nel periodo di cui al paragrafo 2, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione del sistema di IA sul mercato nazionale, per ritirare il prodotto dal mercato o per richiamarlo. Tale autorità notifica senza indebito ritardo la Commissione e gli altri Stati membri di tale misure.

6. La notifica di cui al paragrafo 5 include tutti i particolari disponibili, soprattutto le informazioni necessarie all'identificazione del sistema di IA non conforme, la sua origine, la natura della presunta non conformità e dei rischi connessi, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dal pertinente operatore. Le autorità di vigilanza del mercato indicano in particolare se la non conformità sia dovuta a una o più delle cause seguenti:

-a) non conformità del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5;

a) mancato rispetto da parte di un sistema di IA ad alto rischio dei requisiti di cui al titolo III, capo 2;

b) carenze nelle norme armonizzate o nelle specifiche comuni, di cui agli articoli 40 e 41, che conferiscono la presunzione di conformità.

c) non conformità alle disposizioni di cui all'articolo 52;

d) non conformità dei sistemi di IA per finalità generali ai requisiti e agli obblighi di cui all'articolo 4 bis;

7. Le autorità di vigilanza del mercato degli Stati membri diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano senza indebito ritardo alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del sistema di IA interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.

8. Se, entro tre mesi dal ricevimento della notifica di cui al paragrafo 5, uno Stato membro o la Commissione non sollevano obiezioni contro la misura provvisoria adottata da uno Stato membro, tale misura è ritenuta giustificata. Ciò non pregiudica i diritti procedurali dell'operatore interessato in conformità all'articolo 18 del regolamento (UE) 2019/1020. Il periodo di cui al primo comma del presente paragrafo è ridotto a 30 giorni in caso di non conformità al divieto delle pratiche di intelligenza artificiale di cui all'articolo 5.

9. Le autorità di vigilanza del mercato garantiscono quindi che siano adottate senza indebito ritardo adeguate misure restrittive in relazione al sistema di AI interessato, come il ritiro del prodotto dal loro mercato.

Articolo 66

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 65, paragrafo 5, o entro 30 giorni in caso di non conformità al divieto delle pratiche di intelligenza artificiale di cui all'articolo 5, uno Stato membro solleva obiezioni contro la misura adottata da un altro Stato membro, o se la Commissione ritiene che la misura sia contraria al diritto dell'Unione, la Commissione consulta senza indebito ritardo l'autorità di vigilanza del mercato dello Stato membro e l'operatore o gli operatori pertinenti e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione decide se la misura nazionale sia giustificata o meno entro nove mesi, o 60 giorni in caso di non conformità al divieto delle pratiche di intelligenza artificiale di cui all'articolo 5, a decorrere dalla notifica di cui all'articolo 65, paragrafo 5. Essa notifica tale decisione allo Stato membro interessato. La Commissione informa anche tutti gli altri Stati membri di tale decisione.

2. Se la Commissione ritiene giustificata la misura adottata dall'autorità di vigilanza del mercato dello Stato membro interessato, le autorità di vigilanza del mercato di tutti gli Stati membri provvedono affinché siano adottate misure restrittive appropriate in relazione al sistema di IA interessato, come il ritiro del sistema di IA dal loro mercato senza indebito ritardo, e ne informano la Commissione. Se la misura nazionale è ritenuta ingiustificata dalla Commissione, l'autorità di vigilanza del mercato dello Stato membro interessato provvede a ritirarla e ne informa la Commissione.

3. Se la misura nazionale è ritenuta giustificata e la non conformità del sistema di IA viene attribuita alle carenze nelle norme armonizzate o nelle specifiche comuni di cui agli articoli 40 e 41 del presente regolamento, la Commissione applica la procedura di cui all'articolo 11 del regolamento (UE) n. 1025/2012.

Articolo 67

Sistemi di IA ad alto rischio o per finalità generali conformi che presentano un rischio

1. Se, dopo aver effettuato una valutazione a norma dell'articolo 65, l'autorità di vigilanza del mercato di uno Stato membro ritiene che, sebbene conforme al presente regolamento, il sistema di IA ad alto rischio o per finalità generali presenti un rischio per la salute o la sicurezza delle persone o per i diritti fondamentali, essa chiede all'operatore pertinente di adottare tutte le misure adeguate a far sì che il sistema di IA in questione, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio o che sia ritirato dal mercato o richiamato senza indebito ritardo entro un termine da essa prescritto.

2. Il fornitore o altri operatori pertinenti garantiscono l'adozione di misure correttive nei confronti di tutti i sistemi di IA interessati che hanno messo a disposizione sul mercato in tutta l'Unione entro il termine prescritto dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Lo Stato membro informa immediatamente la Commissione e gli altri Stati membri. Tali informazioni comprendono tutti i dettagli disponibili, in particolare i dati necessari all'identificazione del sistema di IA interessato, l'origine e la catena di approvvigionamento del sistema di IA, la natura del rischio connesso, nonché la natura e la durata delle misure nazionali adottate.

4. La Commissione avvia senza indebito ritardo consultazioni con gli Stati membri interessati e l'operatore o gli operatori pertinenti e valuta le misure nazionali adottate. In base ai risultati di tale valutazione, la Commissione decide se la misura sia giustificata o meno e propone, ove necessario, misure appropriate.

5. La Commissione trasmette la propria decisione agli Stati membri interessati e informa tutti gli altri Stati membri.

Articolo 68

Non conformità formale

1. Un'autorità di vigilanza del mercato di uno Stato membro che giunga a una delle conclusioni riportate di seguito chiede a fornitore pertinente di porre fine alla non conformità contestata entro un termine da essa prescritto:

   a) la marcatura di conformità è stata apposta in violazione dell'articolo 49;

   b) la marcatura di conformità non è stata apposta;

   c) la dichiarazione di conformità UE non è stata redatta;

   d) la dichiarazione di conformità UE non è stata redatta correttamente;

   e) il numero di identificazione dell'organismo notificato coinvolto nella procedura di valutazione della conformità, ove applicabile, non è stato apposto.

2. Se la non conformità di cui al paragrafo 1 permane, lo Stato membro interessato adotta tutte le misure appropriate per limitare o proibire la messa a disposizione sul mercato del sistema di IA ad alto rischio o garantisce che sia richiamato o ritirato dal mercato.

Articolo 68 bis

Impianti di prova dell'Unione nel settore dell'intelligenza artificiale

1. La Commissione designa uno o più impianti di prova dell'Unione a norma dell'articolo 21 del regolamento (UE) 2019/1020 nel settore dell'intelligenza artificiale.

2. Fatte salve le attività degli impianti di prova dell'Unione di cui all'articolo 21, paragrafo 6, del regolamento (UE) 2019/1020, gli impianti di prova dell'Unione di cui al paragrafo 1 forniscono anche pareri tecnici o scientifici indipendenti su richiesta del comitato o delle autorità di vigilanza del mercato.

Articolo 68 ter

Gruppo centrale di esperti indipendenti

1. Su richiesta del comitato per l'IA, la Commissione adotta, mediante atti di esecuzione, disposizioni relative alla creazione, al mantenimento e al finanziamento di un gruppo centrale di esperti indipendenti a sostegno delle attività di contrasto a norma del presente regolamento.

2. Gli esperti sono selezionati dalla Commissione e inclusi nel gruppo centrale sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'intelligenza artificiale, tenendo debitamente conto dei settori tecnici coperti dai requisiti e dagli obblighi di cui al presente regolamento e delle attività delle autorità di vigilanza del mercato a norma dell'articolo 11 del regolamento (UE) 2019/1020. La Commissione determina il numero di esperti del gruppo in funzione delle esigenze.

3. Gli esperti possono svolgere i seguenti compiti:

a) fornire consulenza e sostegno al lavoro delle autorità di vigilanza del mercato, su richiesta di queste ultime;

b) sostenere le indagini transfrontaliere di vigilanza del mercato di cui all'articolo 58, lettera h), fatti salvi i poteri delle autorità di vigilanza del mercato;

c) fornire consulenza e sostegno alla Commissione nello svolgimento delle sue funzioni nell'ambito della clausola di salvaguardia di cui all'articolo 66.

4. Gli esperti svolgono i loro compiti con imparzialità e obiettività e garantiscono la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività. Ogni esperto compila una dichiarazione degli interessi, che rende accessibile al pubblico. La Commissione istituisce sistemi e procedure per gestire attivamente e prevenire potenziali conflitti di interesse.

5. Gli Stati membri possono essere tenuti a pagare tariffe per la consulenza e il sostegno degli esperti. La struttura e il livello delle tariffe, nonché l'entità e la struttura delle spese ripetibili sono adottati dalla Commissione mediante l'atto di esecuzione di cui al paragrafo 1, tenendo conto degli obiettivi di adeguata attuazione del presente regolamento, efficacia in termini di costi e necessità di garantire un accesso effettivo agli esperti da parte di tutti gli Stati membri.

6. 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 dagli impianti di prova dell'Unione a norma dell'articolo 68 bis e dagli esperti a norma del presente articolo sia organizzata in modo efficiente e fornisca il miglior valore aggiunto possibile.

TITOLO IX

CODICI DI CONDOTTA

Articolo 69

Codici di condotta per l'applicazione volontaria di requisiti specifici

1. La Commissione e gli Stati membri agevolano l'elaborazione di codici di condotta intesi a incoraggiare l'applicazione volontaria ai sistemi di IA diversi dai sistemi di IA ad alto rischio di uno o più dei requisiti di cui al titolo III, capo 2 del presente regolamento nella misura del possibile, tenendo conto delle soluzioni tecniche disponibili che consentono l'applicazione di tali requisiti.

2. La Commissione e gli Stati membri agevolano l'elaborazione di codici di condotta intesi a incoraggiare l'applicazione volontaria a tutti i sistemi di IA dei requisiti specifici relativi, ad esempio, alla sostenibilità ambientale, anche per quanto riguarda la programmazione efficiente sotto il profilo energetico, all'accessibilità per le persone con disabilità, alla partecipazione dei portatori di interessi alla progettazione e allo sviluppo dei sistemi di IA e alla diversità dei gruppi che si occupano dello sviluppo sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi. La Commissione e gli Stati membri agevolano inoltre, se del caso, l'elaborazione di codici di condotta applicabili su base volontaria per quanto riguarda gli obblighi degli utenti in relazione ai sistemi di IA.

3. I codici di condotta applicabili su base volontaria possono essere elaborati da singoli fornitori di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione degli utenti e di tutti gli altri portatori di interessi e delle loro organizzazioni rappresentative, ovvero, se del caso, dagli utenti con riguardo ai loro obblighi. 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 cui al presente articolo, la Commissione e gli Stati membri tengono conto degli interessi e delle esigenze specifici delle PMI fornitrici, comprese le start-up.

TITOLO X

RISERVATEZZA E SANZIONI

Articolo 70

Riservatezza

1. In conformità del diritto dell'Unione o nazionale, le autorità nazionali competenti, gli organismi notificati, la Commissione, il comitato e le altre persone fisiche o giuridiche che partecipano all'applicazione del presente regolamento mettono in atto misure tecniche e organizzative adeguate per garantire la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, in particolare:

a) i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, tranne i casi cui si applica l'articolo 5 della direttiva 2016/943 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti;

b) l'efficace attuazione del presente regolamento, in particolare per quanto riguarda ispezioni, indagini e audit;

c) gli interessi pubblici e di sicurezza nazionale;

d) l'integrità del procedimento penale o amministrativo;

e) l'integrità delle informazioni classificate conformemente al diritto dell'Unione o nazionale.

2. Fatto salvo il paragrafo 1, nel momento in cui i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, sono utilizzati dalle autorità di contrasto o dalle autorità competenti in materia di controllo delle frontiere, di immigrazione o di asilo, le informazioni scambiate in via riservata tra le autorità nazionali competenti e tra le autorità nazionali competenti e la Commissione non sono divulgate senza previa consultazione dell'autorità nazionale competente e dell'utente che hanno prodotto tali informazioni, qualora tale divulgazione rischi di compromettere gli interessi pubblici e di sicurezza nazionale. Tale obbligo di scambio di informazioni non riguarda i dati operativi sensibili in relazione alle attività delle autorità di contrasto o in materia di controllo delle frontiere, immigrazione o di asilo.

   Qualora le autorità di contrasto o le autorità competenti in materia di immigrazione o di asilo siano fornitori di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, la documentazione tecnica di cui all'allegato IV rimane nei locali di tali autorità. Tali autorità garantiscono che le autorità di vigilanza del mercato di cui all'articolo 63, paragrafi 5 e 6, a seconda dei casi, possano, su richiesta, accedere immediatamente alla documentazione o ottenerne una copia. Solo il personale dell'autorità di vigilanza del mercato in possesso di un nulla osta di sicurezza di livello adeguato è autorizzato ad accedere a tale documentazione o a una copia della stessa.

3. I paragrafi 1 e 2 non pregiudicano i diritti e gli obblighi della Commissione, degli Stati membri e delle rispettive autorità pertinenti nonché degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, anche nel contesto della cooperazione transfrontaliera, né gli obblighi delle parti interessate di fornire informazioni a norma del diritto penale degli Stati membri.

Articolo 71

Sanzioni

1. Nel rispetto dei termini e delle condizioni di cui al presente regolamento, gli Stati membri stabiliscono le regole relative alle sanzioni, comprese le sanzioni amministrative pecuniarie, applicabili in caso di violazione del presente regolamento e adottano tutte le misure necessarie per garantirne un'attuazione corretta ed efficace. Le sanzioni previste sono effettive, proporzionate e dissuasive. Esse tengono conto in particolare della dimensione e degli interessi delle PMI fornitrici, comprese le start-up, e della loro sostenibilità economica. Esse tengono inoltre conto del fatto che l'uso del sistema di IA avvenga nel contesto di un'attività personale non professionale o meno.

2. Gli Stati membri notificano senza indugio alla Commissione tali norme e misure così come ogni eventuale modifica successiva che le riguardi.

3. La non conformità a uno qualsiasi dei divieti delle pratiche di intelligenza artificiale di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 30 000 000 EUR o, se l'autore del reato è una società, fino al 6 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Nel caso delle PMI, comprese le start-up, tali sanzioni ammontano fino al 3 % del loro fatturato mondiale annuo dell'esercizio precedente.

4. Le violazioni delle seguenti disposizioni connesse a operatori o organismi notificati sono soggette a sanzioni amministrative pecuniarie fino a 20 000 000 EUR o, se l'autore del reato è una società, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

-a) gli obblighi dei fornitori a norma degli articoli 4 ter e 4 quater;

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

b) gli obblighi di talune altre persone a norma dell'articolo 23 bis;

c) gli obblighi dei rappresentati autorizzati a norma dell'articolo 25;

d) gli obblighi degli importatori a norma dell'articolo 26;

e) gli obblighi dei distributori a norma dell'articolo 27;

f) gli obblighi degli utenti a norma dell'articolo 29, paragrafi da 1 a 6 bis;

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

h) gli obblighi di trasparenza per i fornitori e gli utenti a norma dell'articolo 52.

Nel caso delle PMI, comprese le start-up, tali sanzioni ammontano fino al 2 % del loro fatturato mondiale annuo dell'esercizio precedente.

5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR o, se l'autore del reato è una società, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Nel caso delle PMI, comprese le start-up, tali sanzioni ammontano fino all'1 % del loro fatturato mondiale annuo dell'esercizio precedente.

6. Nel decidere l'importo della sanzione amministrativa pecuniaria in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:

a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

a bis) il carattere doloso o colposo della violazione;

a ter) qualsiasi iniziativa adottata dall'operatore al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

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

b bis) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre normative dell'Unione o nazionali, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente atto;

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

d) 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.

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

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

9. L'esercizio da parte dell'autorità di vigilanza del mercato dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

Articolo 72

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

1. Il Garante europeo della protezione dei dati può infliggere sanzioni amministrative pecuniarie alle istituzioni, agli organi e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento. 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 si tiene quanto segue in debita considerazione:

   a) la natura, la gravità e la durata della violazione e delle sue conseguenze;

   b) la cooperazione con il Garante europeo della protezione dei dati al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, compreso il rispetto delle misure precedentemente disposte dal Garante europeo della protezione dei dati nei confronti dell'istituzione, dell'organo o dell'organismo dell'Unione in relazione allo stesso tema;

   c) eventuali precedenti violazioni analoghe commesse dall'istituzione, dall'organo o dall'organismo dell'Unione.

2. La non conformità a uno qualsiasi dei divieti delle pratiche di intelligenza artificiale di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 500 000 EUR.

3. La non conformità del sistema di IA ai requisiti o agli obblighi previsti dal presente regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 250 000 EUR.

4. Prima di adottare qualsiasi decisione a norma del presente articolo, il Garante europeo della protezione dei dati dà all'istituzione, all'organo o all'organismo dell'Unione oggetto del procedimento avviato dal Garante europeo della protezione dei dati l'opportunità di esprimersi in merito all'eventuale violazione. Il Garante europeo della protezione dei dati basa le sue decisioni solo sugli elementi e le circostanze in merito ai quali le parti interessate sono state poste in condizione di esprimersi. Gli eventuali ricorrenti sono strettamente associati al procedimento.

5. Nel corso del procedimento sono pienamente garantiti i diritti di difesa delle parti interessate. Esse hanno diritto d'accesso al fascicolo del Garante europeo della protezione dei dati, fermo restando l'interesse legittimo delle persone fisiche o delle imprese alla tutela dei propri dati personali o segreti aziendali.

6. I fondi raccolti mediante l'imposizione di sanzioni pecuniarie in forza del presente articolo entrano nel bilancio generale dell'Unione.

TITOLO XI

DELEGA DI POTERE E PROCEDURA DI COMITATO

Articolo 73

Esercizio della delega

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

2. La delega di potere di cui all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, e all'articolo 48, paragrafo 5, è conferita alla Commissione per un periodo di cinque anni a decorrere dal [*data di entrata in vigore del presente regolamento*].

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 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, e all'articolo 48, paragrafo 5, 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. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

5. Qualsiasi atto delegato adottato a norma dell'articolo 7, paragrafi 1 e 3, dell'articolo 11, paragrafo 3, dell'articolo 43, paragrafi 5 e 6, e dell'articolo 48, paragrafo 5, 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 74

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

TITOLO XII

DISPOSIZIONI FINALI

Articolo 75

Modifica del regolamento (CE) n. 300/2008

All'articolo 4, paragrafo 3, del regolamento (CE) n. 300/2008 è aggiunto il comma seguente:

"Nell'adottare misure dettagliate relative alle specifiche tecniche e alle procedure per l'approvazione e l'uso delle attrezzature di sicurezza per quanto concerne i sistemi di intelligenza artificiale ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 76

Modifica del regolamento (UE) n. 167/2013

All'articolo 17, paragrafo 5, del regolamento (UE) n. 167/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 77

Modifica del regolamento (UE) n. 168/2013

All'articolo 22, paragrafo 5, del regolamento (UE) n. 168/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...).";

Articolo 78

Modifica della direttiva 2014/90/UE

All'articolo 8 della direttiva 2014/90/UE è aggiunto il paragrafo seguente:

"4. Per i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, nello svolgimento delle sue attività a norma del paragrafo 1 e nell'adottare specifiche tecniche e norme di prova conformemente ai paragrafi 2 e 3, la Commissione tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 79

Modifica della direttiva (UE) 2016/797

All'articolo 5 della direttiva (UE) 2016/797 è aggiunto il paragrafo seguente:

"12. Nell'adottare atti delegati a norma del paragrafo 1 e atti di esecuzione a norma del paragrafo 11 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 80

Modifica del regolamento (UE) 2018/858

All'articolo 5 del regolamento (UE) 2018/858 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti delegati a norma del paragrafo 3 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 81

Modifica del regolamento (UE) 2018/1139

Il regolamento (UE) 2018/1139 è così modificato:

1) all'articolo 17 è aggiunto il paragrafo seguente:

"3. Fatto salvo il paragrafo 2, nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

2) all'articolo 19 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

3) all'articolo 43 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

4) all'articolo 47 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

5) all'articolo 57 è aggiunto il paragrafo seguente:

"Nell'adottare tali atti di esecuzione per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale], si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.";

6) all'articolo 58 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento."

Articolo 82

Modifica del regolamento (UE) 2019/2144

All'articolo 11 del regolamento (UE) 2019/2144 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti di esecuzione a norma del paragrafo 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) YYY/XX [sull'intelligenza artificiale] del Parlamento europeo e del Consiglio*, si tiene conto dei requisiti di cui al titolo III, capo 2, di tale regolamento.

_____

* Regolamento (UE) YYY/XX [sull'intelligenza artificiale] (GU...)."

Articolo 83

Sistema di IA già immessi sul mercato o messi in servizio

1. Il presente regolamento non si applica ai sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato IX che sono stati immessi sul mercato o messi in servizio prima del [*12 mesi dopo la data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*], a meno che la sostituzione o la modifica di tali atti giuridici non comporti una modifica significativa della progettazione o della finalità prevista del sistema di IA o dei sistemi di IA interessati.

   Si tiene conto dei requisiti di cui al presente regolamento, ove applicabile, nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato IX da effettuare come previsto in tali atti.

2. Il presente regolamento si applica ai sistemi di IA ad alto rischio, diversi da quelli di cui al paragrafo 1, che sono stati immessi sul mercato o messi in servizio prima del [*data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*], solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione o finalità prevista.

Articolo 84

Valutazione e riesame

1. [soppresso]

1 ter. La Commissione valuta la necessità di modificare l'elenco di cui all'allegato III ogni 24 mesi dopo l'entrata in vigore del presente regolamento e fino al termine del periodo della delega di potere. I risultati di tale valutazione sono presentati al Parlamento europeo e al Consiglio.

2. Entro [*tre anni dalla data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*] e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento. Le relazioni sono rese pubbliche.

3. Le relazioni di cui al paragrafo 2 dedicano particolare attenzione ai seguenti aspetti:

   a) lo stato delle risorse finanziarie, delle attrezzature tecniche e delle risorse umane necessarie alle autorità nazionali competenti per lo svolgimento efficace dei compiti loro assegnati a norma del presente regolamento;

   b) lo stato delle sanzioni, in particolare delle sanzioni amministrative pecuniarie di cui all'articolo 71, paragrafo 1, applicate dagli Stati membri in caso di violazione delle disposizioni del presente regolamento.

4. Entro [*tre anni dalla data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2*] e successivamente ogni quattro anni, se del caso, la Commissione valuta l'impatto e l'efficacia dei codici di condotta volontari per la promozione dell'applicazione dei requisiti di cui al titolo III, capo 2, per i sistemi di IA diversi dai sistemi di IA ad alto rischio ed eventualmente di altri requisiti supplementari per i sistemi di IA, anche per quanto riguarda la sostenibilità ambientale.

5. Ai fini dei paragrafi da 1 bis a 4, il comitato, gli Stati membri e le autorità nazionali competenti forniscono alla Commissione informazioni su sua richiesta.

6. Nello svolgere le valutazioni e i riesami di cui ai paragrafi da 1 bis a 4, la Commissione tiene conto delle posizioni e delle conclusioni del comitato, del Parlamento europeo, del Consiglio, nonché di altri organismi o fonti pertinenti.

7. Se necessario, la Commissione presenta opportune proposte di modifica del presente regolamento tenendo conto, in particolare, degli sviluppi delle tecnologie e alla luce dei progressi della società dell'informazione.

Articolo 85

Entrata in vigore e applicazione

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

2. Il presente regolamento si applica a decorrere dal [36 mesi dopo l'entrata in vigore del regolamento].

3. In deroga al paragrafo 2:

   a) il titolo III, capo 4, e il titolo VI si applicano a decorrere da [12 mesi dopo l'entrata in vigore del presente regolamento];

   b) l'articolo 71 si applica a decorrere dal [12 mesi dopo l'entrata in vigore del regolamento].

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

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente / La presidente	*Il presidente*

ALLEGATO I

[soppresso]

ALLEGATO II

ELENCO DELLA NORMATIVA DI ARMONIZZAZIONE DELL'UNIONE

Sezione A – Elenco della normativa di armonizzazione dell'Unione in base al nuovo quadro normativo

1. Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24) [abrogata dal regolamento sui prodotti macchina];

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 imbarcazioni 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

1. 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);

2. 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);

3. 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);

4. 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);

5. 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);

6. 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);

7. 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);

8. 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.

ALLEGATO III

SISTEMI DI IA AD ALTO RISCHIO DI CUI ALL'ARTICOLO 6, PARAGRAFO 3

In ciascuno dei settori elencati ai punti da 1 a 8, i sistemi di IA specificamente menzionati a ciascuna lettera sono considerati sistemi di IA ad alto rischio ai sensi dell'articolo 6, paragrafo 3.

1. Biometria:

   a) i sistemi di identificazione biometrica remota.

2. Infrastrutture critiche:

   a) i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale e della fornitura di acqua, gas, riscaldamento ed 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 o ai programmi 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 o programmi di istruzione o 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) l'IA destinata a essere utilizzata per adottare decisioni in materia di promozione e cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali e 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 autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, 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 messi in servizio per uso proprio da fornitori che sono microimprese, piccole imprese e medie imprese ai sensi dell'allegato della raccomandazione 2003/361/CE della Commissione;

c) i sistemi di IA destinati a essere utilizzati per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi vigili del fuoco e assistenza medica;

d) 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, a eccezione dei sistemi di IA messi in servizio per uso proprio da fornitori che sono microimprese, piccole imprese e medie imprese ai sensi dell'allegato della raccomandazione 2003/361/CE della Commissione.

6. Attività di contrasto:

a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto per determinare il rischio di reato o recidiva in relazione a una persona fisica o il rischio per una persona fisica di diventare una vittima potenziale di reati;

b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;

c) [soppresso]

d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;

e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto per prevedere il verificarsi o il ripetersi di un reato effettivo o potenziale 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;

f) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto 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.

g) [soppresso]

7. Gestione della migrazione, dell'asilo e del controllo delle frontiere:

a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, come poligrafi e strumenti analoghi, o per rilevare lo stato emotivo di una persona fisica;

b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto 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) [soppresso]

d) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto per esaminare le domande di asilo, di visto e di permesso di soggiorno e i relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status.

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 interpretare i fatti o il diritto e per applicare la legge a una serie concreta di fatti.

ALLEGATO IV

DOCUMENTAZIONE TECNICA di cui all'articolo 11, paragrafo 1

La documentazione tecnica di cui all'articolo 11, paragrafo 1, deve includere almeno le seguenti informazioni, a seconda dell'applicabilità al pertinente sistema di IA.

1. Una descrizione generale del sistema di IA comprendente:

   a) la finalità prevista, la persona o le persone che sviluppano il sistema, la data e la versione del sistema;

   b) il modo in cui il sistema interagisce o può essere utilizzato per interagire con hardware o software che non fanno parte del sistema di IA stesso, ove applicabile;

   c) le versioni dei pertinenti software o firmware e qualsiasi requisito relativo all'aggiornamento della versione;

   d) la descrizione di tutte le forme in cui il sistema di IA è immesso sul mercato o messo in servizio (per es. pacchetto software incorporato nell'hardware, scaricabile, API, ecc.);

   e) la descrizione dell'hardware su cui è destinato a operare il sistema di IA;

   f) se il sistema di IA è un componente di prodotti, le fotografie o le illustrazioni che mostrino le caratteristiche esterne, la marcatura e il layout interno di tali prodotti;

   g) le istruzioni per l'uso destinate all'utente e, ove applicabile, le istruzioni per l'installazione.

2. Una descrizione dettagliata degli elementi del sistema di IA e del processo relativo al suo sviluppo, compresi:

   a) i metodi applicati e le azioni eseguite per lo sviluppo del sistema di IA, compresi, ove opportuno, il ricorso a sistemi o strumenti preaddestrati forniti da terzi e il modo in cui sono stati utilizzati, integrati o modificati dal fornitore;

b) le specifiche di progettazione del sistema, vale a dire la logica generale del sistema di IA e degli algoritmi; le principali scelte di progettazione, comprese le motivazioni e le ipotesi formulate, anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato; le principali scelte di classificazione; gli aspetti che il sistema è progettato per ottimizzare e la pertinenza dei diversi parametri; la descrizione dell'output atteso del sistema; le decisioni in merito a eventuali compromessi posti in essere con riguardo alle soluzioni tecniche adottate per soddisfare i requisiti di cui al titolo III, capo 2;

c) la descrizione dell'architettura del sistema che spiega in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo; le risorse computazionali utilizzate per sviluppare, addestrare, sottoporre a prova e convalidare il sistema di IA;

d) ove pertinente, i requisiti in materia di dati mediante schede tecniche che descrivono le metodologie e le tecniche di addestramento e i set di dati di addestramento utilizzati, comprese una descrizione generale di tali set di dati e le informazioni sulla loro origine, sul loro ambito di applicazione e sulle loro principali caratteristiche; le modalità di ottenimento e di selezione dei dati; le procedure di etichettatura, ad esempio per l'apprendimento supervisionato, e le metodologie di pulizia dei dati, ad esempio il rilevamento di valori anomali (outlier);

e) la valutazione delle misure di sorveglianza umana necessarie in conformità dell'articolo 14, compresa una valutazione delle misure tecniche necessarie per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti, in conformità dell'articolo 13, paragrafo 3, lettera d);

f) ove applicabile, una descrizione dettagliata delle modifiche predeterminate del sistema di IA e delle sue prestazioni, unitamente a tutte le informazioni pertinenti relative alle soluzioni tecniche adottate per garantire la conformità costante del sistema di IA ai requisiti pertinenti di cui al titolo III, capo 2;

g) le procedure di convalida e di prova utilizzate, comprese le informazioni sui dati di convalida e di prova utilizzati e sulle loro principali caratteristiche; le metriche utilizzate per misurare l'accuratezza, la robustezza, la cibersicurezza e la conformità ad altri requisiti pertinenti di cui al titolo III, capo 2, nonché gli impatti potenzialmente discriminatori; i log delle prove e tutte le relazioni di prova corredate di data e firma delle persone responsabili, anche per quanto riguarda le modifiche predeterminate di cui alla lettera f).

3. Informazioni dettagliate sul monitoraggio, sul funzionamento e sul controllo del sistema di IA, in particolare per quanto riguarda: le sue capacità e limitazioni in termini di prestazioni, compresi i gradi di accuratezza relativi a determinate persone o determinati gruppi di persone sui quali il sistema è destinato a essere utilizzato e il livello di accuratezza complessivo atteso in relazione alla finalità prevista del sistema; i prevedibili risultati indesiderati e fonti di rischio per la salute, la sicurezza e i diritti fondamentali, nonché di rischio di discriminazione in considerazione della finalità prevista del sistema di IA; le misure di sorveglianza umana necessarie in conformità dell'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti; le specifiche relative ai dati di input, se del caso.

4. Una descrizione dettagliata del sistema di gestione dei rischi in conformità dell'articolo 9.

5. Una descrizione delle modifiche pertinenti apportate dal fornitore al sistema durante il suo ciclo di vita.

6. Un elenco delle norme armonizzate applicate integralmente o in parte i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea; nei casi in cui tali norme armonizzate non sono state applicate, una descrizione dettagliata delle soluzioni adottate per soddisfare i requisiti di cui al titolo III, capo 2, compreso un elenco delle altre norme e specifiche tecniche pertinenti applicate.

7. Una copia della dichiarazione di conformità UE.

8. Una descrizione dettagliata del sistema predisposto per valutare le prestazioni del sistema di IA nella fase successiva all'immissione sul mercato in conformità dell'articolo 61, compreso il piano di monitoraggio successivo all'immissione sul mercato di cui all'articolo 61, paragrafo 3.

ALLEGATO V
DICHIARAZIONE DI CONFORMITÀ UE

La dichiarazione di conformità UE di cui all'articolo 48 deve contenere tutte le seguenti informazioni:

1. il nome e il tipo del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;

2. il nome e l'indirizzo del fornitore o, ove applicabile, del suo rappresentante autorizzato;

3. un'attestazione secondo cui la dichiarazione di conformità UE è rilasciata sotto la responsabilità esclusiva del fornitore;

4. un'attestazione secondo cui il sistema di IA in questione è conforme al presente regolamento e, ove applicabile, a qualsiasi altra pertinente normativa dell'Unione che preveda il rilascio di una dichiarazione di conformità UE;

5. i riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune in relazione alla quale è dichiarata la conformità;

6. ove applicabile, il nome e il numero di identificazione dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato;

7. il luogo e la data di rilascio della dichiarazione, il nome e la funzione della persona che firma la dichiarazione nonché un'indicazione della persona a nome e per conto della quale ha firmato, la firma.

ALLEGATO VI

PROCEDURA DI VALUTAZIONE DELLA CONFORMITÀ BASATA SUL CONTROLLO INTERNO

1. La procedura di valutazione della conformità basata sul controllo interno è la procedura di valutazione della conformità basata sui punti da 2 a 4.

2. Il fornitore verifica la conformità del sistema di gestione della qualità istituito ai requisiti di cui all'articolo 17.

3. Il fornitore esamina le informazioni contenute nella documentazione tecnica al fine di valutare la conformità del sistema di IA ai pertinenti requisiti essenziali di cui al titolo III, capo 2.

4. Il fornitore verifica inoltre che il processo di progettazione e sviluppo del sistema di IA e il monitoraggio successivo alla sua immissione sul mercato di cui all'articolo 61 siano coerenti con la documentazione tecnica.

ALLEGATO VII

CONFORMITÀ BASATA SULLA VALUTAZIONE DEL SISTEMA DI GESTIONE DELLA QUALITÀ E SULLA VALUTAZIONE DELLA DOCUMENTAZIONE TECNICA

1. Introduzione

La conformità basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica scaturisce dalla procedura di valutazione della conformità di cui ai punti da 2 a 5.

2. Aspetti generali

Il sistema di gestione della qualità approvato per la progettazione, lo sviluppo e la prova dei sistemi di IA a norma dell'articolo 17 deve essere esaminato conformemente al punto 3 e deve essere soggetto alla vigilanza di cui al punto 5. La documentazione tecnica del sistema di IA deve essere esaminata conformemente al punto 4.

3. Sistema di gestione della qualità

3.1. La domanda presentata dal fornitore deve comprendere:

a) il nome e l'indirizzo del fornitore e, nel caso in cui la domanda sia presentata dal rappresentante autorizzato, anche il nome e l'indirizzo di quest'ultimo;

b) l'elenco dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;

c) la documentazione tecnica di ciascuno dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;

d) la documentazione relativa al sistema di gestione della qualità che deve contemplare tutti gli aspetti elencati all'articolo 17;

e) una descrizione delle procedure vigenti per garantire che il sistema di gestione della qualità rimanga adeguato ed efficace;

f) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato.

3.2. Il sistema di gestione della qualità deve essere valutato dall'organismo notificato, che deve stabilire se soddisfa i requisiti di cui all'articolo 17.

La decisione deve essere notificata al fornitore o al suo rappresentante autorizzato.

Tale notifica deve indicare le conclusioni della valutazione del sistema di gestione della qualità e la decisione di valutazione motivata.

3.3. Il sistema di gestione della qualità approvato deve continuare a essere attuato e mantenuto dal fornitore in modo da rimanere adeguato ed efficiente.

3.4. Il fornitore deve portare all'attenzione dell'organismo notificato qualsiasi modifica prevista del sistema di gestione della qualità approvato o dell'elenco dei sistemi di IA cui si applica tale sistema.

Le modifiche proposte devono essere esaminate dall'organismo notificato, che deve decidere se il sistema di gestione della qualità modificato continua a soddisfare i requisiti di cui al punto 3.2 o se è necessaria una nuova valutazione.

L'organismo notificato deve notificare al fornitore la propria decisione. Tale notifica deve indicare le conclusioni dell'esame e la decisione di valutazione motivata.

4. Controllo della documentazione tecnica

4.1. Oltre alla domanda di cui al punto 3, il fornitore deve presentare una domanda a un organismo notificato di propria scelta per la valutazione della documentazione tecnica relativa al sistema di IA che il fornitore intende immettere sul mercato o mettere in servizio e cui si applica il sistema di gestione della qualità di cui al punto 3.

4.2. La domanda deve comprendere:

a) il nome e l'indirizzo del fornitore;

b) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato;

c) la documentazione tecnica di cui all'allegato IV.

4.3. La documentazione tecnica deve essere esaminata dall'organismo notificato. Se del caso e nei limiti di quanto necessario per lo svolgimento dei suoi compiti, all'organismo notificato deve essere concesso pieno accesso ai set di dati di addestramento, convalida e prova utilizzati, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso interfacce di programmazione delle applicazioni (API) o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.

4.4. Nell'esaminare la documentazione tecnica, l'organismo notificato può chiedere al fornitore di presentare elementi probatori supplementari o di eseguire ulteriori prove per consentire una corretta valutazione della conformità del sistema di IA ai requisiti di cui al titolo III, capo 2. Ogniqualvolta non è soddisfatto delle prove effettuate dal fornitore, l'organismo notificato stesso deve effettuare prove adeguate, a seconda dei casi.

4.5. Agli organismi notificati è concesso l'accesso al codice sorgente del sistema di IA su richiesta motivata e solo qualora siano soddisfatte le seguenti condizioni cumulative:

a) l'accesso al codice sorgente è necessario per valutare la conformità del sistema di IA ad alto rischio ai requisiti di cui al titolo III, capo 2; e

b) le procedure di prova e di audit e le verifiche basate sui dati e sulla documentazione presentati dal fornitore sono state esperite o si sono dimostrate insufficienti.

4.6. La decisione deve essere notificata al fornitore o al suo rappresentante autorizzato. Tale notifica deve indicare le conclusioni della valutazione della documentazione tecnica e la decisione di valutazione motivata.

Se il sistema di IA è conforme ai requisiti di cui al titolo III, capo 2, l'organismo notificato deve rilasciare un certificato di valutazione UE della documentazione tecnica. Tale certificato deve indicare il nome e l'indirizzo del fornitore, le conclusioni dell'esame, le eventuali condizioni di validità e i dati necessari per identificare il sistema di IA.

Il certificato e i suoi allegati devono contenere tutte le informazioni pertinenti per consentire la valutazione della conformità del sistema di IA e il controllo del sistema di IA durante l'uso, ove applicabile.

Se il sistema di IA non è conforme ai requisiti di cui al titolo III, capo 2, l'organismo notificato deve rifiutare il rilascio di un certificato di valutazione UE della documentazione tecnica e deve informare in merito il richiedente, motivando dettagliatamente il suo rifiuto.

Se il sistema di IA non soddisfa il requisito relativo ai dati utilizzati per l'addestramento, sarà necessario addestrare nuovamente il sistema di IA prima di presentare domanda per una nuova valutazione della conformità. In tal caso, la decisione di valutazione motivata dell'organismo notificato che rifiuta il rilascio del certificato di valutazione UE della documentazione tecnica contiene considerazioni specifiche sui dati di qualità utilizzati per formare il sistema di IA, in particolare sui motivi della non conformità.

4.7. Qualsiasi modifica del sistema di IA che potrebbe incidere sulla conformità ai requisiti o sulla finalità prevista dello stesso deve essere approvata dall'organismo notificato che ha rilasciato il certificato di valutazione UE della documentazione tecnica. Il fornitore deve informare tale organismo notificato quando intende introdurre una delle modifiche di cui sopra o quando viene altrimenti a conoscenza del verificarsi di tali modifiche. Le modifiche previste devono essere valutate dall'organismo notificato, che deve decidere se esse rendono necessaria una nuova valutazione della conformità a norma dell'articolo 43, paragrafo 4, o se possono essere gestite tramite un supplemento del certificato di valutazione UE della documentazione tecnica. In quest'ultimo caso, l'organismo notificato deve valutare le modifiche, notificare al fornitore la propria decisione e, in caso di approvazione delle modifiche, rilasciare a quest'ultimo un supplemento del certificato di valutazione UE della documentazione tecnica.

5. Vigilanza del sistema di gestione della qualità approvato

5.1. La finalità della vigilanza a cura dell'organismo notificato di cui al punto 3 è garantire che il fornitore rispetti debitamente i termini e le condizioni del sistema di gestione della qualità approvato.

5.2. Ai fini della valutazione, il fornitore deve consentire all'organismo notificato di accedere ai locali in cui hanno luogo la progettazione, lo sviluppo e le prove dei sistemi di IA. Il fornitore deve inoltre condividere con l'organismo notificato tutte le informazioni necessarie.

5.3. L'organismo notificato deve eseguire audit periodici per assicurarsi che il fornitore mantenga e applichi il sistema di gestione della qualità e deve trasmettere al fornitore una relazione di audit. Nel contesto di tali audit, l'organismo notificato può effettuare prove supplementari dei sistemi di IA per i quali è stato rilasciato un certificato di valutazione UE della documentazione tecnica.

ALLEGATO VIII

INFORMAZIONI DA PRESENTARE ALL'ATTO DELLA REGISTRAZIONE DI OPERATORI E DI SISTEMI DI IA AD ALTO RISCHIO IN CONFORMITÀ DELL'ARTICOLO 51

I fornitori, i rappresentanti autorizzati e gli utenti che sono autorità, agenzie o organismi pubblici presentano le informazioni di cui alla parte I. I fornitori o, se del caso, i rappresentanti autorizzati garantiscono che le informazioni sui loro sistemi di IA ad alto rischio di cui alla parte II, punti da 1 a 11, siano complete, corrette e aggiornate. Le informazioni di cui al punto II.12 sono generate automaticamente dalla banca dati.

Parte I. Informazioni relative agli operatori (all'atto della registrazione degli operatori)

-1. Il tipo di operatore (fornitore, rappresentante autorizzato o utente);

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

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

Parte II. Informazioni relative al sistema di IA ad alto rischio

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

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

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

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

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

6. 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;

7. una copia scannerizzata del certificato di cui al punto 6, ove applicabile;

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

9. una copia della dichiarazione di conformità UE di cui all'articolo 48;

10. le istruzioni per l'uso in formato elettronico;

11. un indirizzo internet per ulteriori informazioni (facoltativo);

12. il nome, l'indirizzo e i dati di contatto degli utenti.

ALLEGATO VIII bis

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 54 BIS

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione alle prove in condizioni reali che devono essere registrate a norma dell'articolo 54 bis:

1. il numero di identificazione unico a livello dell'Unione della prova in condizioni reali;

2. il nome e i dati di contatto del fornitore o potenziale fornitore e degli utenti coinvolti nella prova in condizioni reali;

3. una breve descrizione del sistema di IA, la sua finalità prevista e altre informazioni necessarie per l'identificazione del sistema;

4. una sintesi delle principali caratteristiche del piano di prova in condizioni reali;

5. informazioni sulla sospensione o sulla cessazione della prova in condizioni reali.

ALLEGATO IX

NORMATIVA DELL'UNIONE SUI SISTEMI IT SU LARGA SCALA NELLO SPAZIO DI LIBERTÀ, SICUREZZA E GIUSTIZIA

1. Sistema di informazione Schengen

   a) Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018, pag. 1);

   b) regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 (GU L 312 del 7.12.2018, pag. 14);

   c) regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

2. Sistema di informazione visti

   a) Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (CE) n. 767/2008, il regolamento (CE) n. 810/2009, il regolamento (UE) 2017/2226, il regolamento (UE) 2016/399, il regolamento (UE) 2018/XX [regolamento sull'interoperabilità] e la decisione 2004/512/CE, e che abroga la decisione 2008/633/GAI del Consiglio (COM(2018) 302 final). Da aggiornare dopo l'adozione del regolamento (aprile/maggio 2021) da parte dei colegislatori.

3. Eurodac

a) Proposta modificata di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che istituisce l'"Eurodac" per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) XXX/XXX [regolamento sulla gestione dell'asilo e della migrazione] e del regolamento (UE) XXX/XXX [regolamento sul reinsediamento], per l'identificazione di cittadini di paesi terzi o apolidi il cui soggiorno è irregolare e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 (COM (2020) 614 final).

4. Sistema di ingressi/uscite

a) Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011 (GU L 327 del 9.12.2017, pag. 20).

5. Sistema europeo di informazione e autorizzazione ai viaggi

a) Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1);

b) regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (GU L 236 del 19.9.2018, pag. 72).

6. Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi

   a) Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).

7. Interoperabilità

   a) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27);

   b) regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).